Independent Security Assessment — Phase II Preparedness Guide

Assessed entities guide to:

- Pre-Assessment Preparation
- On-Site Configuration Requirements
- Assessment Requirements
- Post-Assessment Delivery

Version 3.4, dated 5/22/2019
Previous editions are obsolete

Legal Notice and Disclaimer:

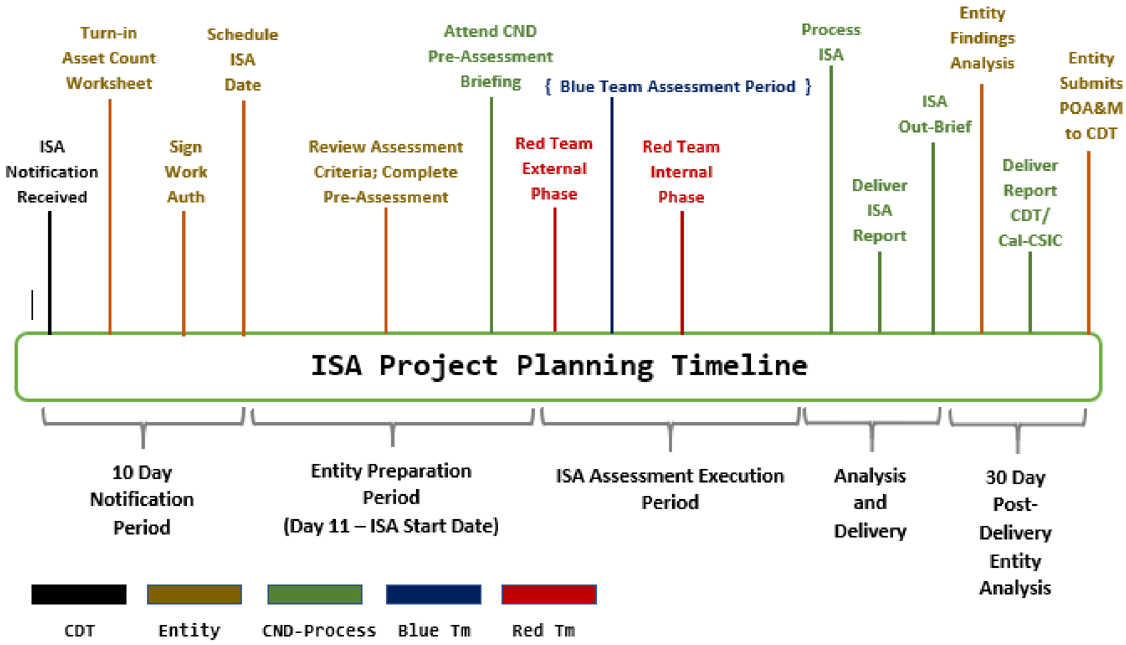
Please note that much of this publication is based on prior professional experience and anecdotal evidence. Although the author and organization have made every reasonable attempt to achieve complete accuracy of the content in this guide, they assume no responsibility for errors or omissions. Also, you should use this information in accordance with your existing internal security protocols and practices. Follow these instructions at your own risk. Your situation may not be exactly suited to the examples illustrated here as every entity's network is unique. If you have questions on how to proceed, please contact the CND Engagement Manager for assistance at 916-854-4CND (4263) or via email at info@cnd.ca.gov.

Any trademarks, service marks, product names or named features are assumed to be the property of their respective owners and are used only for reference. There is no implied endorsement of said products or services.

Contents

Introduction to Preparing for the Independent Security Assessment (ISA)

The Preparedness Guide provides the entity an overview of the steps necessary to achieve the best potential and positive outcome when undergoing an Independent Security Assessment. The assessment goal is to provide an external party view of the entity's current cybersecurity state and to provide recommendations for improvement. The assessment analyzes a series of technical controls as designated by the State Chief Information Security Officer (CISO). To ensure a smooth process with the least amount of impact to the entity's staff, a series of pre-assessment preparation steps are provided within this guide. Due to the constrained timeline for each ISA, the entity's overall results can be negatively impacted if the entity be ill prepared. To assist in the planning and execution, a general timeline is provided (Figure 1). Using the timeline and this guide, entities undergoing a CND provided ISA can more accurately plan, prepare, and successfully execute the ISA process. The entity should review and follow this guide in its entirety to gain the maximum potential benefit from the assessment.



ISA Notification Received
Turn-in Asset Count Worksheet
Sign Work Auth
Schedule ISA Date
Review Assessment Criteria; Complete Pre-Assessment
Attend CND Pre-Assessment Briefing
Red Team External Phase
{ Blue Team Assessment Period }
Red Team Internal Phase
Process ISA
Deliver ISA Report
ISA Out-Brief
Entity Findings Analysis
Deliver Report CDT/ Cal-CSIC
Entity Submits POA&M to CDT
ISA Project Planning Timeline
10 Day Notification Period
Entity Preparation Period (Day 11 – ISA Start Date)
ISA Assessment Execution Period
Analysis and Delivery
30 Day Post-Delivery Entity Analysis
CDT
Entity
CND-Process
Blue Tm
Red Tm

Figure 1. General Timeline for Successful ISA Participation

Two Team Approach

The ISA as performed by the CND is conducted using a two-team approach. One team performs the Defensive Assessment portion and the other performs the Offensive Assessment (Penetration test). These teams are referred to through this guide as the Assessment team (Blue Team) and the Penetration Test Team (Red Team). These two teams operate independently of each other and conduct operations at different intervals (detailed later in this document).

Blue Team (Assessment Team): The Blue Team is responsible for conducting the tasks associated with network defense and hardening. They are the entity's trusted assistance team. The entity will be sharing configuration and credentials with the Blue Team during the ISA process. Credentials, accesses, and configuration information provided to the Blue Team is not shared with the Red Team. The Blue Team Leader performs as the CND's on-site liaison between the Entity Liaison and the CND staff.

The Blue Team operations begin upon their initial arrival at the entity site. Their tasks include a comprehensive vulnerability assessment, analysis of the public website, firewall rules analysis, measurement of system hardening, 24-hour network traffic capture, various NIST related logical checks related to account management and FIPS compliance implementation, and they measure phishing resistance. Phishing resistance is the only offensive task the Blue Team conducts.

Note: Blue Team phishing measures the targeted user's ability to detect and report phishing emails to their organization cybersecurity management team. At no time will the Blue Team attempt to deploy malicious code to the users. If the Blue Team successfully collects credentials from the target users, they are not shared with the Red Team.

Red Team (Penetration Test Team): The Red Team represents a group of threat actors whom have targeted the entity's network for possible network compromise and data theft. Do not share credentials or defensive configuration information with the Red Team members. On a typical engagement, you will not interact with the Red Team. If the entity attempts to interact with a Red Team member to share information that is intended for the Blue Team, they will be stopped and redirected to the Blue Team Lead. There are three exceptions of interaction between the entity and the Red Team:

1. Significant Risk: The Red Team will take a *"Hard Pause"* if it detects a risk so significant that delayed disclosure is likely to result in loss of confidentiality, integrity, or availability by a real-world threat actor. A hard pause is an immediate halt of all actions conducted by the Red Team on the identified resource and is immediate confidential reporting to the entity liaison. The Red Team will immediately disclose the risk to the Entity Liaison for the risk to be addressed by the entity to reduce the possibility of potential compromise.

2. Illegal Activity: If the CND detects the potential presence of illegal activity (external threat actor compromise, insider threat activities, etc.) the ISA will initiate a *"Hard Sto*p". The Red/Blue Team leads will work with the entity to document its findings for enclosure in the required entity-initiated Cal-CSIRS report. The Hard Stop will remain in effect until the CHP Cyber Crimes team releases the network for continued CND actions. This could result in the ISA being rescheduled to another available date in the ISA calendar.

3. Malicious Activity Detection: Entity security staff is encouraged to disclose to the Red Team when malicious activity is detected. This provides the entity an opportunity to validate their security tools are tuned to provide the appropriate level of detection and alerting. The Red Team will work with the security team regarding next steps of resulting detections. In some cases, the entity may choose to not block the action to allow the red team time to complete testing a potential risk.

Penetration Test Phases:

The Penetration Test portion of the ISA is divided into two testing phases – external and internal penetration testing.

External Phase: During the external phase, the Red Team operates offsite. Operations typically begin on the first day of the ISA (unless otherwise coordinated in advance). During the external phase, the Red Team simulates a typical commodity threat actor. During this segment, the Red Team will:

- Collect meta-data and other publicly available materials that could be used to spear-phish members, probe and scan for service exposure, abuse susceptible service exposures, attempt to obtain a foothold on entity assets, escalate permissions on hosts, and acquire sensitive access.
- Conduct separate Red Team directed Spear-phishing event(s) (see Appendix D for rules of engagement). Red Team spear-phishing may include the introduction of specially crafted malware designed to create a foothold on the entity's hosts.

Internal Phase: During the internal phase, the Red Team is on-site. The first day of the internal penetration testing begins immediately following the last day of the external penetration testing and is conducted on the entity's internal network. During the internal phase, the Red Team simulates an insider threat. The Red Team conducts similar actions to the external phase and introduces man-in-the-middle simulations as well at other credential theft techniques. The one exception in tactics that is not internally performed is spear phishing.

Key Roles within this Guide

While every entity is different, CND recognizes there are functional roles that are typically standardized within state government. For clarity, the presumed roles are defined below in Table 1. Entities should map the roles defined to the appropriate individuals in their organization to ensure the appropriate actions are accomplished within the necessary timeframes. The guide provides a tasks-list based on generally accepted functional roles in a typical Information Technology organization.

Table 1. Key Roles

Roles	Description	Notes
Senior Cybersecurity Manager (SCM)	Senior cybersecurity manager within the organization. This role is typically assigned the role of daily security operations management and retains oversight of cybersecurity defense actions and change management within the organization. This can be the CIO, ISO, etc. He/she will be the Assessment coordinator for the ISA and the Primary POC for all coordination efforts with the CND.	Do not delegate this role. Delegation of this role could place your assessment at-risk of lower performance.
Senior Network Administrator (NA)	Senior member of the Network Administration team with hands-on access to network infrastructure devices. He/she has change management and configuration change approval.	
Senior System Administrator (SA)	Senior member of the Systems Administration team with hands-on access to host configuration change and account creation/management.	If this role is divided between Windows and Linux teams, then the senior individual from the Windows/Linux teams will be assigned to this role.
Service Desk Manager (SDM)	Manager with oversight to the call center, support desk, and other client initial points of technical assistance.	If SDM does not control phishing notice release, the individual responsible should be included as well.
Entity Liaison (EL)	Primary on-site interface person between Blue/Red Teams and the entity. Except for extreme cases, this should be one person.	This person should be technical and have change control notification. This can be the SCM in smaller entities.

Guide Dissemination

The Preparedness Guide is designed to help the assessed entity prepare for a successful engagement. It is critical that this document be disseminated internally to the responsible individuals within the assessed entity that will be engaged in the pre-assessment, assessment, and post-assessment activities.

The **Entity Liaison** is responsible to ensure the entity's efforts achieve the desired state of readiness prior to the assessment start date. Delays, missing documentation, or absent staff prevent the assessment team from rendering a complete assessment in the time frame allotted and may result in 'Non-compliance' findings. Please help the CND assist the entity to gain the most benefit possible by ensuring entity readiness for assessment.

Preparing for an Independent Security Assessment

The ISA is a technical analysis that indicates the entity's current cybersecurity maturity. Unlike an audit, all tasks under assessment are technical in nature. The entity should use this document and the provided Independent Security Assessment Criteria as a guideline for preparing for the assessment. It is recommended that the entity performs their own internal assessment to identify shortfalls that should be remediated to meet overall compliance and a higher state of cybersecurity.

Note: The criteria for the ISA is under the control of the CISO office. While CND is an authorized provider, it is not authorized to make changes or modifications to the standards or measures. The ISA Criteria is accessible through the CDT website at https://cdt.ca.gov/security/independent-security-assessments-services/.

Planning for Staff Impact

The CND recognizes staff time is valuable and limited. This guide leverages multiple years of assessment experience to provide insight in obtaining the highest state of readiness while lowering the impact on the staff to the minimum level possible. Staff impact depends upon the entity's level of technical expertise, current cybersecurity practices, access to funding, and existing documentation. To assist in minimizing impacts during the assessment, the following guidance should be adhered to:

- Defer network changes during the Assessment Window (do not schedule any major hardware/software upgrades and/or replacements)
- Entity should avoid conducting sweeping security deployments just prior to the ISA window
- Ensure Key Role team members who will be involved in the assessment are not scheduled for extended leave during the ISA window

Pre-Assessment Section

The pre-assessment portion details all tasks that should occur prior to the ISA start date. Day notations are recommendations. It is the entity's responsibility to ensure proper assignment and execution of all actions to ensure the necessary outcomes are completed prior to the required Section (Pre-Assessment, Assessment). However, CND will review your status of the tasks completed.

Task Role Cross-Reference

- Organizational Chief Information Security Officer or ISO if none assigned (CIO)
- Senior Cybersecurity Manager (SCM)
- Senior Network Administrator (NA)
- Senior System Administrator (SA)
- Service Desk Manager (SDM)

Task	Roles	Task Detail	Days Prior to Pre-Assessment Briefing Date	Completed
1	CIO	Designate SCM. Provide contact information on Tab 2 of the Data Call Worksheet (see Appendix A)	50+	
2	CIO	Designate Entity Liaison. Provide contact info on Tab 2 of the Data Call Worksheet	50+	
3	SCM	Self-Identify to CND Engagement Manager via email (see Appendix G)	50+	
4	SCM	Distribute Preparedness Guide to individuals who are assigned roles within the assessment / guide	50+	
5	SCM	A. Coordinate the ISA Pre-Assessment Briefing with CND Engagement Manager B. Upon receipt from the CND Engagement Manager, forward the Pre-Assessment Briefing calendar invite to Entity key roles and stakeholders	45+	
6	SA	Identify website owners (see Appendix B). Complete Tab 6 of the Data Call Worksheet	45+	
7	SA	Notify 3rd party hosts for externally hosted web applications/sites and document approval	45+	
8	NA	Identify externally accessible public IP space and resources. Complete Tab 4 of the Data Call Worksheet (see Appendix A)	25+	
9	SCM	Identify nominated phishing participants. Complete Tab 7 of the Data Call Worksheet (see Appendix C)	25+	
10	NA	Identify internally used IP space and resources. Complete Tab 5 of the Data Call Worksheet (see Appendix A)	20+	
11	SCM /NA	Identify a workspace for the CND team for the entire period of assessment. Co-locate teams (when possible) to reduce entity requirements. Workspace must meet the following requirements: • Accommodate 4-6 personnel • Deploy a switch with 8 dedicated cat5/6 data jacks with at least 100Mbps each (see Task 21 assigned	20+	

		to Network Admin) • Afford privacy from common space (e.g. Conference Room) and secure with a lock		
12	SCM	A. Coordinate ISA Kick-off Meeting with CND Engagement Manager and invite Entity key roles (Infosec Management. System Admin, Network Admin, Entity Liaison). Include CND Engagement Manager in the meeting invite. B. Schedule conference room for meeting location	20+	
13	NA	A. Identify any network blocking technology (ACL, Firewall rules, IPS, etc.) between management subnet and all hosts on network B. Implement measures to enable Blue Team scanners access to **all** Entity Systems.	20+	
14	SA	A. Identify any host-based blocking technology (HIPS, AV, etc.) between management subnet and all hosts on network **(Blue Team ports only)** B. Coordinate with NA to implement measures to mitigate via Group Membership, VLAN, or other security methods	20+	
15	SCM	Verify status of readiness. Collect concerns/questions in preparation for ISA Pre-Assessment Briefing	18+	
16	SCM	Identify sensitive data contents that would require entity's immediate notification if detected by CND externally (e.g. SSNs, account numbers, key words, technologies, etc.). Disclose at Pre-Assessment Briefing	18+	
17	SCM	Submit Data Call Worksheet to CND Engagement Manager (info@cnd.ca.gov)	17+	
18	SA	Ensure the following host services are available for Vulnerability scanning (SSH may have to be enabled for scanning purposes on Linux and mac systems): Windows: tcp/135,137,139,445 Unix/Linux/Mac: tcp/22 Notes: (1) This is a Blue Team operation. If modifying how these services are exposed to the network, ensure those modifications are only presented to the subnet the Blue Team operates from. (2) Unless otherwise restricted, these services are typically available as part of normal host management operations. Always validate prior to the ISA.	17+	
19	SCM /SA/ NA	Review ISA Criteria and understand what will be assessed. Write down any questions in preparation for the Pre-Assessment Briefing. Notify appropriate parties to be prepared to present proof to ISA team when requested.	10+	
20	SCM	A. Attend ISA Pre-Assessment Briefing B. Provide an update on the status of all tasks on the Pre-Assessment Task List C. Track remaining tasks and questions D. Identify critical concern data exposures E. Ensure all organizational requirements are completed prior to ISA start date	10+	

Task	Role	Task Detail	Days Prior to Asmt Start Date	Completed
21	NA	Configure switch with the provided ISA space for the following requirements: Blue Team: 4 ports Management VLAN (Mandatory) Red Team: 4 ports in the entity's highest user density VLAN; ports should issue IP's like a normal use receives (e.g. DHCP) The ISA teams use multiple Virtual hosts, Disable ALL Port Security and IP issue restrictions are removed from this switch (Mandatory). If the Network Administrator has questions, please contact CND no less than 7 days prior. ** Please mark the ports as Blue / Red	10+	
22	NA	IP access requirements: Blue Team: Issue 4 DHCP or static IP addresses (entity preference). Regardless of how these are issued they must be Whitelisted in your endpoint protection, IDS/IPS technology.. Red Team: 6 IP's to be issued via DHCP. Note: Do not take any special actions (e.g. whitelisting of Red-team address space. Provide access to normal user subnets.	10+	
23	SA	A. Identify 10 hosts by host name and IP address (3 workstations, 3 laptops, 3 Application Servers, and 1 Domain Controller) for system hardening assessment B. Provide list of target hosts to SCM	10+	
24	SCM	Validate all required key roles will be present for ISA	10+	
25	NA	Provide network interconnection diagram to SCM for Blue Team documentation	8+	
26	SA	• Prepare accounts for Blue Team: • 2 X Domain Admin Accounts -- Best Practice: Copy a known good Domain Admin account and rename (see below for naming convention) • 1 X Standard User Account • Account Naming Convention Standard: Must start with "CND_" (IE: CND_1, CND_2, CND_3). • Accounts need to be in currently used OUs. Do not create a special OU for these accounts. • This helps to ensure Red Team does not leverage provided accounts against entity • If more than one domain is present - prepare for all domains • Non-Domain Joined Assets: Local System Admin Account for each asset Identify which Local Admin Accts work with which assets to prevent account lockout • Non-Windows Hosts: Provide Root-level credentials for Mac's, Linux, AIX, Unix hosts Identify	8+	

		which Local Admin Accts work with which assets to prevent account lockout. **TEST DOMAIN ADMIN ACCOUNTS AFTER CREATION**		
27	SA	• Whitelist CND provider IP address for phishing campaign (see Appendix D)	3+	
28	SA	Disable and verify Sleep/Power Saver functions to disabled to prevent host unavailability during off hours. There are no exceptions for this requirement!	3+	
29	NA	Establish span port to mirror egress/ingress network traffic between Inside of firewall and network core switch in preparation for the 24-hour network traffic capture	3+	
30	NA	Deploy/test access switch in designated workspace for Blue/Red Team usage (previously configured in Task 20)	1	
31	EL	Ensure Blue/Red Team have proper building/parking access to facility (Identify if access badges are required)	1	

Assessment Section

This section details all the tasks that occur during the ISA Assessment phase.

Task Role Cross-Reference:

- Organizational Chief Information Security Officer or ISO if none assigned (CIO)
- Senior Cybersecurity Manager (SCM)
- Senior Network Administrator (NA)
- Senior System Administrator (SA)
- Service Desk Manager (SDM)
- Entity Liaison (EL)

Task #	Assigned Individual	Task Detail	Completed
1	EL	During external penetration testing and prior to Blue Team arrival, notify CND Engagement Manager of unusual activities detected by network admin/system admin to determine if they were initiated by Red Team or other activities (see Appendix C, Figure 1.)	
2	SCM	Ensure all designated attendees attend the ISA Kick-off Meeting	
3	SCM	Deliver any updates/materials not previously delivered to Blue Team Lead during ISA Kick-off meeting (see Appendix E)	
4	SCM/EL	Ensure Blue Team Leader has appropriate contact info, workspace access and network access	
5	EL	Notify Blue Team Leader of any Phishing Campaigns detected prior to entity response/action. Note: If CND identifies the detected phishing campaign as part of Blue Team actions, the entity should not take action. If CND identifies the phishing campaign as a Red Team tactic, then the entity should take appropriate action **except notify Cal-CSIRS**	
6	EL	Notify Blue Team of unusual activities detected by network admin/system admin to determine if they were initiated by Red-Team or other activities	
7	NA	Facilitate assistance to have Firewall Administrator generate required configuration files for delivery to Blue Team Leader	
8	SCM/EL	Coordinate with Red Team in event of hard pause	
9	EL	Coordinate with internal technical defensive teams for left-seat/right-seat, advisory and assistance opportunity (as appropriate)	

Post-Assessment Section

This section entails all the tasks that occur during the post ISA Assessment phase.

Task Role Cross-Reference:

- CND Engagement Manager (CEM)
- Senior Cybersecurity Manager (SCM)
- Entity Liaison (EL)

Task #	Assigned Individual	Task Detail
1	EL	Coordinate deactivation of badge access, network access/accounts, etc. to fully deprovision CND access
2	SCM	Receive notification of Password Reset for compromised accounts
3	CEM	Notify the entity the final report is ready for delivery and schedule delivery date; send out brief meeting Invite to SCM
4	CEM	Schedule secure electronic delivery of final brief products; provide 1st half of secure decryption password 3-5 days prior to out brief
5	SCM	Forward Out Brief invite to entity key roles and appropriate management team members
6	SCM	Schedule conference room and notify entity key roles and appropriate management team members of location
7	EL	Ensure Skype for Business Meeting (using native client, not web client) is prepared for the Out Brief (see Appendix F)
8	CEM	Initiate Out Brief. Facilitates meeting as required
9	SCM	Following the Out Brief, validate all files are complete and viewable. Request replacements for damaged files (as applicable)
10	SCM	Review results with larger IT teams. Determine courses of action for remediation. Determine timelines
11	SCM	Prepare Plans of Action and Milestones (POA&M) for submission to CDT
12	SCM	Submit POA&M to CDT via secure FTP server (within 30 days)
13	SCM	Update POA&M as required

Appendix - A - Data Call Worksheet Scoping (Tabs 4 & 5)

Tabs 4 & 5 contain some of the most important information the entity provides in the Data Call Worksheet. Providing accurate data will reduce entity time and effort while improving the quality of the ISA results. Tabs 4 & 5 pertain to the Red Team actions.

Purpose: To ensure your assessment provides the highest degree of risk insight, the entity MUST accurately identify all of their information technology (referred to as assets). This due diligence activity is core to the entity's successful participation. To support the ISA activities by both teams and both zones (External and Internal), the Data Call Worksheet provides two Tabs, External and Internal.

Scoping Considerations: Generally, the entity will consider all computer hosts (Servers, Workstations, Desktops, Laptops, and Appliances with an IP address) that the entity has privileged/administrative access, that reside within the entity allocated IP address space or on a 3rd party hosted networks as In-scope. Regardless of scoping, all IP ranges MUST be identified.

- Examples of In-scope hosts:
  - Windows, Unix, Linux, BSD, Apple hosts (workstations, notebooks, laptops, servers, virtual servers, bare metal host, network appliances, thin clients, IoT devices, etc.) that the entity has root or administrator level log-on rights
  - Third-party hosts residing in the Entity IP Address space in which the entity is responsible for the validation of the hosts' security configuration
  - Microsoft Azure / Amazon AWS / etc. cloud hosted domain controllers, file and application servers, web servers
  - 3rd Party web/application servers hosted in non-State of California managed data centers

- Examples of assets potentially eligible for out-of-scope request
  - A host owned by another agency (not covered under this assessment) that the entity does not have configuration management or administrative access.
  - A host that provides life-preserving services, which if rendered off-line for greater than 10 minutes, could result in loss of life, catastrophic financial damage to citizens, or significant damage to property. A detailed justification will be required for these hosts.
  - A host designated critical IT asset that is suffering from stability issues; if unexpected reboots were to occur could result in an unrecoverable condition and loss of data.
  - CDT / Cal-CSIC provided cybersecurity sensors / collectors

****Please note**: At the Entity's option, the Data Call Worksheet may be submitted via encrypted email to CND Engagement Manager. Please coordinate in advance.

Tab 4 – External Scoping:

Steps:

1. Identify all IP addresses externally exposed to the internet. Sources include:

- Advertised IPs by CDT under the entity's control
- External Router Advertisements
- Firewalls

2. Using Tab 4, list each IP range in address blocks no larger than a CIDR Class "C" in size. If only a single IP address is in use, either list it separately or as a x.x.x.x/32 address. The Entity should NOT list a CIDR Block or IP address range larger in a /23 (512 IP's) as a single entry. Entities unable to provide

fine-grain detail on larger IP address blocks will require *intrusive IP Scanning* and may incur additional days of service at additional cost to fulfill the ISA requirements.

3. Requesting an Out-of-Scope for a host is an anomaly event; a typical assessment will not have any approved Out-of-Scope assets. If you believe you have a valid requirement for an Out-of-Scope host, list the asset in the Out of Scope list and prepare documentation to support the out-of-scope request. To reduce complexity, address these issues prior to the Pre-Assessment In-brief with the CND Engagement Manager. The documentation should address the unique issue and the impact to core service delivery of the entity. Once completed, coordinate with the CND Engagement Manager for delivery of the information for review.

4. For assets hosted on non-entity-controlled networks, place an "X" in appropriate Yes or No box adjacent to the entry. Include the date the 3rd part host was notified.

5. In cases where the asset is requested to meet the out-of-scope classification, enter that asset in the Out-of-Scope portion of Tab 4 and submit the justification documentation with your Data Worksheet.

*Note: This includes all DSL Lines, Cable Modems, and other external connection IP addresses.

Tab 5 – Internal Scoping:

Steps:

1. Identify all IP addresses utilized on the internal, VPN, and hosted networks that are not externally accessible. Sources include:

- IP's assigned by CDT, Microsoft Azure, and other cloud providers, which are only accessible from inside the entity network and under entity control
- Internal router advertisements
- Firewalls
- DHCP Scopes
- VPN Tunnels

2. Using Tab 5, list each IP range in address blocks no larger than a CIDR Class "C" in size, and designated its general purpose (e.g. printer subnet, servers, accounting department subnet, etc.). If only a single IP address is in use within the given Class C range, either list it separately or as a x.x.x.x/32 address. The entity should NOT list a CIDR Block or IP address range larger in a /23 (512 IP's) as a single entry. If the entity is unable to provide fine-grain detail on larger IP address blocks, CND will require *intrusive IP scanning* and may incur additional cost to fulfill the ISA requirements.

3. Requesting an Out-of-Scope for a host is an anomaly event; a typical assessment will not have any approved Out-of-Scope assets. If you believe you have a valid requirement for an Out-of-Scope host, list the asset in the Out of Scope list and prepare documentation to support the out-of-scope request. To reduce complexity, address these issues prior to the Pre-Assessment In-brief with the CND Engagement Manager. The documentation should address the unique issue and the impact to core service delivery of the entity. Once completed, coordinate with the CND Engagement Manager for delivery of the information for review.

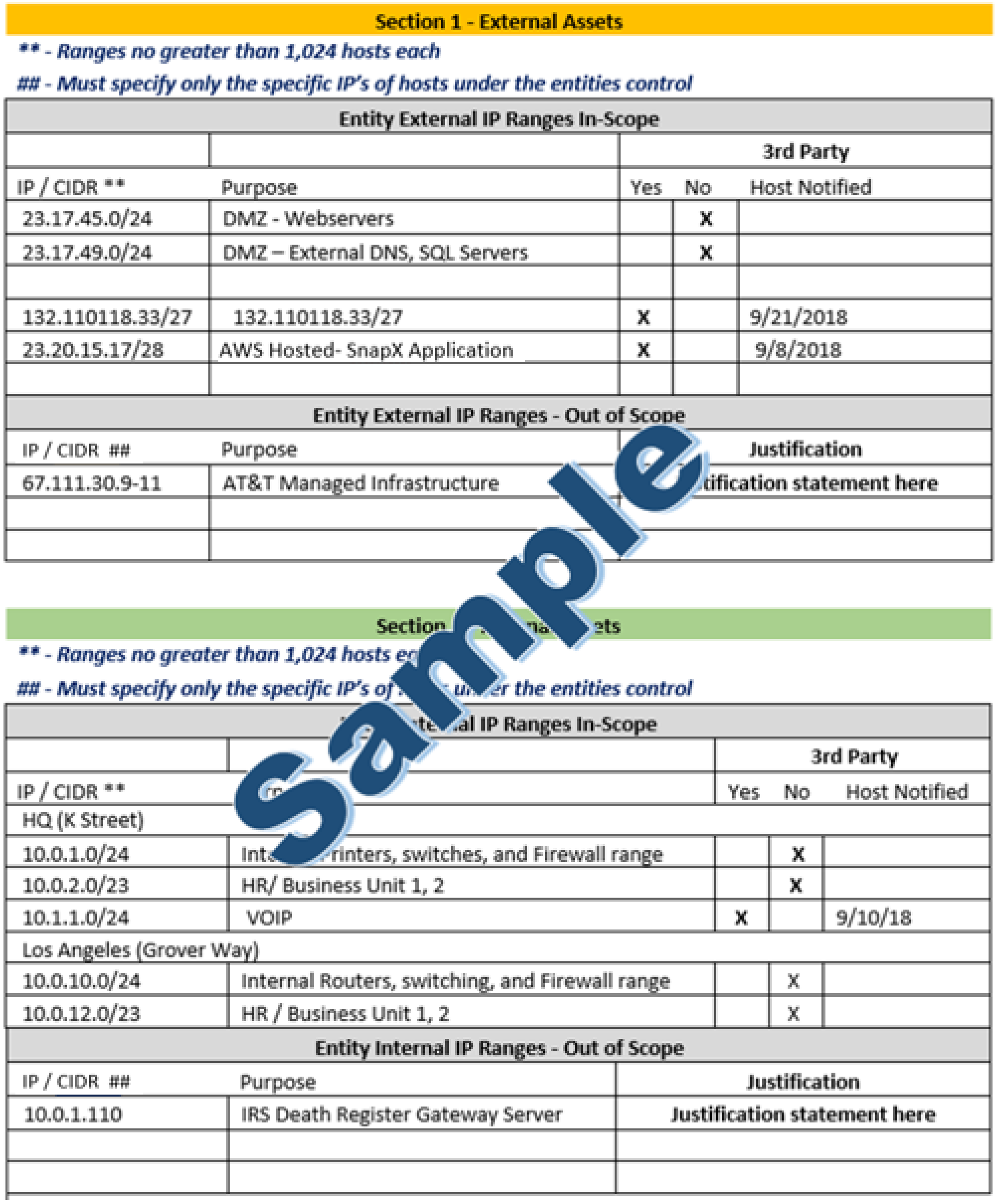
4. For assets hosted on non-entity-controlled networks, place an "X" in appropriate Yes or No box adjacent to the entry. Include the date the 3rd part host was notified.

5. In cases where the asset is requested to meet the out-of-scope classification, enter that asset in the Out-of-Scope portion of Tab 5 and submit the justification documentation with your Data Worksheet.

6. For IP addresses hosted internally for assets not managed by the entity (e.g. another agency not under assessment, leased commercial hosts which the entity has provided a Pentest summary report completed in the past 24 months) the entity may place those IP addresses in the out-of-scope Justification block of Tab 5.

7. Internal IP addresses that are publicly accessible / routable will be scanned from the outside during the external phase.

Scoping Example Entries:



Section 1 - External Assets

***** - Ranges no greater than 1,024 hosts each***

## - Must specify only the specific IP's of hosts under the entities control

Entity External IP Ranges In-Scope				
		3rd Party		
IP / CIDR **	Purpose	Yes	No	Host Notified
23.17.45.0/24	DMZ - Webservers		X	
23.17.49.0/24	DMZ – External DNS, SQL Servers		X	
132.110118.33/27	132.110118.33/27	X		9/21/2018
23.20.15.17/28	AWS Hosted- SnapX Application	X		9/8/2018

Entity External IP Ranges - Out of Scope		
IP / CIDR ##	Purpose	Justification
67.111.30.9-11	AT&T Managed Infrastructure	Justification statement here

Section 2 - Internal Assets

***** - Ranges no greater than 1,024 hosts each***

## - Must specify only the specific IP's of hosts under the entities control

Entity Internal IP Ranges In-Scope				
		3rd Party		
IP / CIDR **	Purpose	Yes	No	Host Notified
HQ (K Street)				
10.0.1.0/24	Internal Printers, switches, and Firewall range		X	
10.0.2.0/23	HR/ Business Unit 1, 2		X	
10.1.1.0/24	VOIP	X		9/10/18
Los Angeles (Grover Way)				
10.0.10.0/24	Internal Routers, switching, and Firewall range		X	
10.0.12.0/23	HR / Business Unit 1, 2		X	

Entity Internal IP Ranges - Out of Scope		
IP / CIDR ##	Purpose	Justification
10.0.1.110	IRS Death Register Gateway Server	Justification statement here

Appendix – B - Web Assessment Site Selection (Tab 6)

Entities may have multiple internet-facing websites. Due to the time-based nature of the assessment, a maximum of 5 publicly assessible web sites will be considered in-scope for the Assessment. The Red-Team may determine additional sites will be targeted for limited penetration testing on an ad-hoc basis.

Purpose: To assist entities prioritize the highest value internet facing web properties, the following criteria should be considered when completing Tab 6 Public Facing Websites:

- Sensitivity of the information processed
- Likelihood of loss of life, property, or financial damage should the host / data processed be compromised
- Age and mitigative measures applied to the host
- The criticality of the host to providing core-services to the entity's constituency

Steps:

1. List all public facing web assets on Tab 6

2. Place the entities public "www" web site as entry # 1 (this site is mandated for assessment)

3. Reorder the remaining sites based on a risk / priority rating on the tab beginning at position # 2.

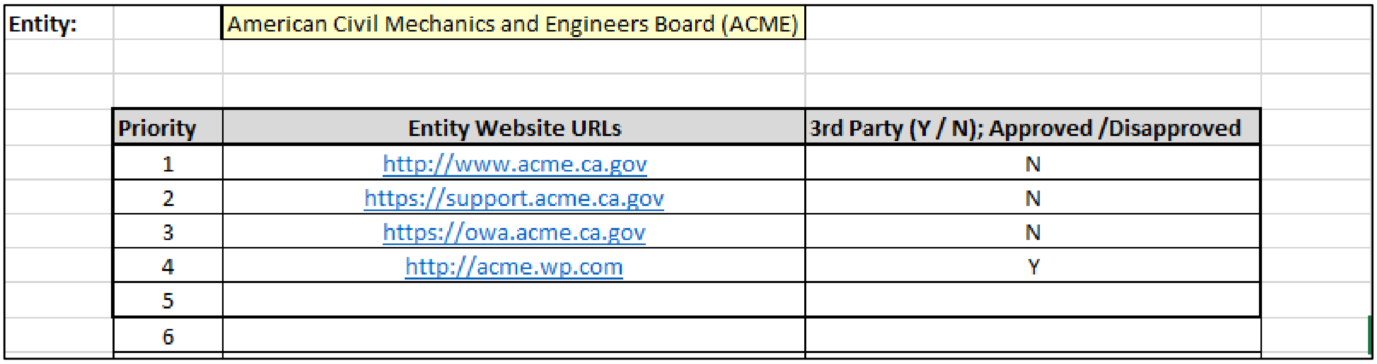
4. If the site is hosted in a Data Center not under the direct control of the entity (CDT, Amazon, etc.) then the entity must follow the hosts established Web Pentest Notification Process. Contact hosting provider for additional information. Once the host provider approval is obtained, enter the data in the "3rd Party Host Approved" column. If the host refuses to allow Pentest, please notify CDT of the non-compliant host so efforts can be made to move your site to a location that meets state compliance standards.

5. Do not list sites that are not accessible from the Internet. Providing a user level password for password protected sites may yield better results but is not required. If a password is provided, the access level should be User and the credentials (Username and Password) placed in column E and F on the line of the site.

6. If the entity has significant concerns about a specific web application / site, please address those directly with the CND Engagement Manager.

NOTE: If you save your web server logs on the same drive as your operating system, there is a chance that repeated analysis could fill the logs and cause your OS drive to run out of space. This is a risky configuration and should be resolved prior to the ISA to help avoid potential outages.

Example Submission:



Entity:		American Civil Mechanics and Engineers Board (ACME)		
	Priority	**Entity Website URLs**	**3rd Party (Y / N); Approved /Disapproved**	
	1	http://www.acme.ca.gov	N	
	2	https://support.acme.ca.gov	N	
	3	https://owa.acme.ca.gov	N	
	4	http://acme.wp.com	Y	
	5			
	6			

Appendix – C - Rules of Engagement, Phishing Events

Purpose: Phishing is the primary real-world method most threat actors achieve their initial foothold on networks. As a result, the ISA approaches this area in two different ways. It is important the entity clearly understands their expected actions under both approaches to ensure successful measurement.

Blue Team Phishing Event/Tasks: Blue Team phishing is designed to measure the effectiveness of user training with regards to the identification of a phishing attacks using modern phishing methods. It is scored in two ways. First, the Blue Team phishing is based on the time required for users to identify a potential phishing threat to the cybersecurity management team. Second, the Blue Team phishing examines the metrics associated with the number of user(s) that perform the following actions related to the message:

- Click the provided link
- Provided Credentials (if applicable)

For the purposes of this event, this is an information collection activity only. Blue Team events NEVER include malicious attachments or other payloads.

Tasks listed below must be accomplished prior to ISA:

- The entity must provide a minimum of 100 users (up to 200 users may be submitted at the entities request) on Tab 7 - Phishing of the Data Call Worksheet. If the entity has less than 100 employees total, submit all employees on Tab 7.
- Submission must include the following data in the provided fields on Tab 7 (First Name, Last Name, Email Address)
- Entity will review the provided names prior submission to ensure all participants are active employees and reasonably expected to be working during ISA assessment period
  - Replace submissions for employees that do not meet the criteria
- The submitted entries must include 3 executives, 3 IT administrators, and the remaining users a mixture from all entity's business units
  - If entity has less than the minimum required employee classes for any given category, than all employees in the category will be provided
- The CIO, AIO, SCM, and other key role team members will be excluded from the submitted entries
- Entity must Whitelist the CND phishing server IP addresses, see Appendix D of this guide for instructions
  - Entities not on O365 email must seek assistance with the vendor to ensure they whitelist the provided email server prior to the assessment period
  - Failing to Whitelist the server or blocking (manually or automated) the phishing server will result in an automatic score of Non-Compliance for violation of the Rules of Engagement

Red Team Spear Phishing Event/Tasks: Red Team events are designed to test the entity's currently deployed security tools and assess their ability to detect and prevent malware payloads, malicious process execution, and C2 network communication. These events may include malicious attachments that utilize specially crafted remote command utilities (implants) that report directly to CND controlled C2 hosts. All implants are designed to dissolve at the end of the engagement and no manual clean-up should be required.

Users for this portion are selected by the Penetration Test Team Leader. Targeted users are identified during the open source data collection phase. As a result, selected users are likely different from those submitted for the Blue Team Phishing Campaign. Users targeted under the Spear Phishing Campaign may receive specially crafted emails with custom payloads designed to emulate an insider threat's attempt to establish a backdoor into the internal entity network. The backdoors are designed to test security controls implementation and will be eliminated upon completion of the test

Rules of Engagement

Expectation upon receipt of a Phishing Email during the Assessment Period: To ensure the entity both preserves the integrity of the assessment while appropriately defending their network, the following Rules of Engagement (RoE) are provided. All actions during the assessment period regarding possible phishing events require interaction with the CND prior to action.

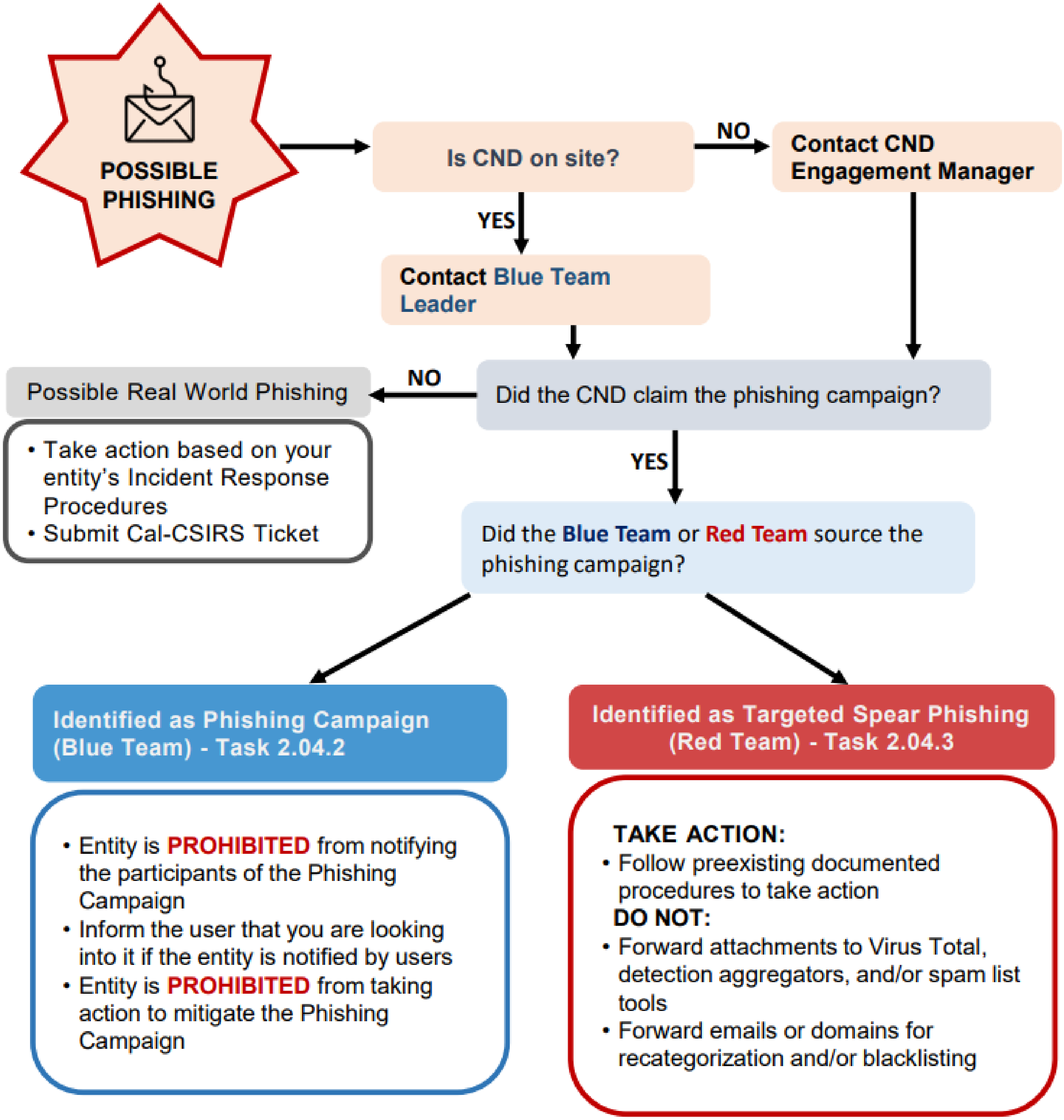
- **Under no circumstances will the entity block any identified CND Domains or IP addresses or report these addresses / IP's to 3rd party spam or Virus Total services!**
- During the ENITRE ISA period, the entity shall report all detected instances of Phishing immediately to the Blue Team Leader. If the Blue Team Leader is not on site, contact the CND Engagement Manager. **Failure to adhere to this requirement could result in task failure for RoE violation.**
    - Blue Team Leader/CND Engagement Manager will: Determine if the Phishing is Blue, Red, or external threat actor generated.
- Blue Team Phishing:
- **Warning --** Blue Team phishing will be logged, and no other action taken. User inquiries will be provided the response "We are researching this issue, you may delete the email from your inbox". No other actions or notifications will be undertaken until the end of the assessment period.
- **Warning –** The entity is prohibited from notifying the participants of the Assessment Phishing Campaign while it is in process. Notifying users will result in a *Non-Compliance (N)* score for the associated event.

- Red Team Phishing:
- Entity is authorized to take any of the following actions once a Red Team Spear-Phishing attempt is identified:
    - Notify users, following preexisting documented procedures
    - Remove the email using preexisting documented procedures
    - Perform any post-analysis process in accordance with preexisting documented procedures
        - Note: **Do NOT** reimage or offline the host, inconveniencing the user. CND C2 malware is strictly controlled by the CND and safe for ISA use
    - **Do NOT** submit samples using manual or automated methods to sandboxing, Malware Analysis, or other defensive tools / sites
    - **Do NOT** submit a report to any external Agencies, CDT (via Cal-CSIRS), or the Cal-CSIC
        - Doing so expends efforts and takes time away from responses to real-world attacks
        - If reporting is a part of your existing process, discuss the actions with your team that you would normally take when reporting the event to the Blue Team Leader

- Verified External Threat Actor generated events will be handled in accordance with the entity's normal protection policies and reported through Cal-CSIRS.

Figure 1.

Phishing Rules of Engagement



POSSIBLE PHISHING
Is CND on site?
NO
Contact CND Engagement Manager
YES
Contact Blue Team Leader
Did the CND claim the phishing campaign?
NO
Possible Real World Phishing
YES
Did the Blue Team or Red Team source the phishing campaign?
Identified as Phishing Campaign (Blue Team) - Task 2.04.2
Identified as Targeted Spear Phishing (Red Team) - Task 2.04.3

- Take action based on your entity's Incident Response Procedures
- Submit Cal-CSIRS Ticket

- Entity is **PROHIBITED** from notifying the participants of the Phishing Campaign
- Inform the user that you are looking into it if the entity is notified by users
- Entity is **PROHIBITED** from taking action to mitigate the Phishing Campaign

TAKE ACTION:

- Follow preexisting documented procedures to take action

DO NOT:

- Forward attachments to Virus Total, detection aggregators, and/or spam list tools
- Forward emails or domains for recategorization and/or blacklisting

Prohibited actions for both campaigns:

- Entity is **PROHIBITED** from blocking any identified CND Domains or IP addresses
- Entity is **PROHIBITED** from submitting phishing campaign samples thru manual or automated methods to sandbox, malware analysis, or other defensive tools/sites
- Entity is **PROHIBITED** to submit a report to any external agencies, CDT (via Cal-CSIRS), or the Cal-CSIC
- Campaign will initiate during normal business hours

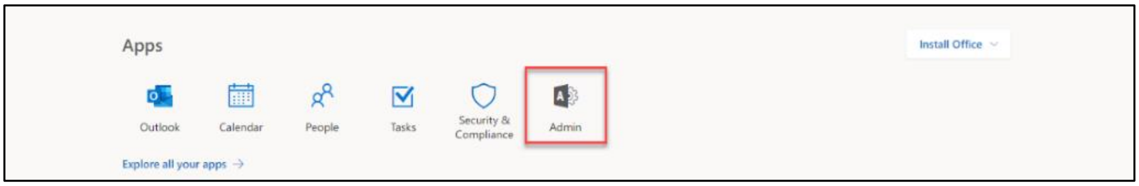
Appendix D - Phishing Whitelisting Procedures

Office 365 Whitelist Phishing Server IP Assessment

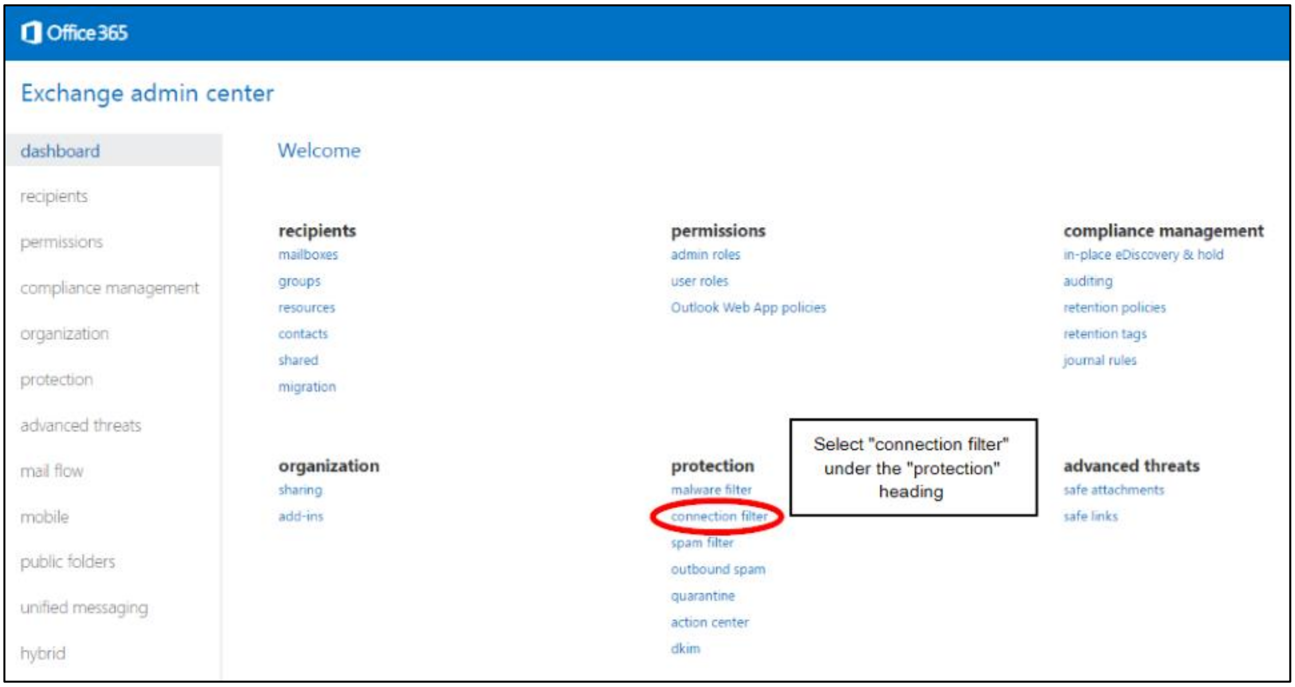
Note: Due to the nature of O365 updates, these screens may change without notice.

Setting Up Your IP Allow List

1. Log into your mail server admin portal and go into the **Admin -> Exchange.**

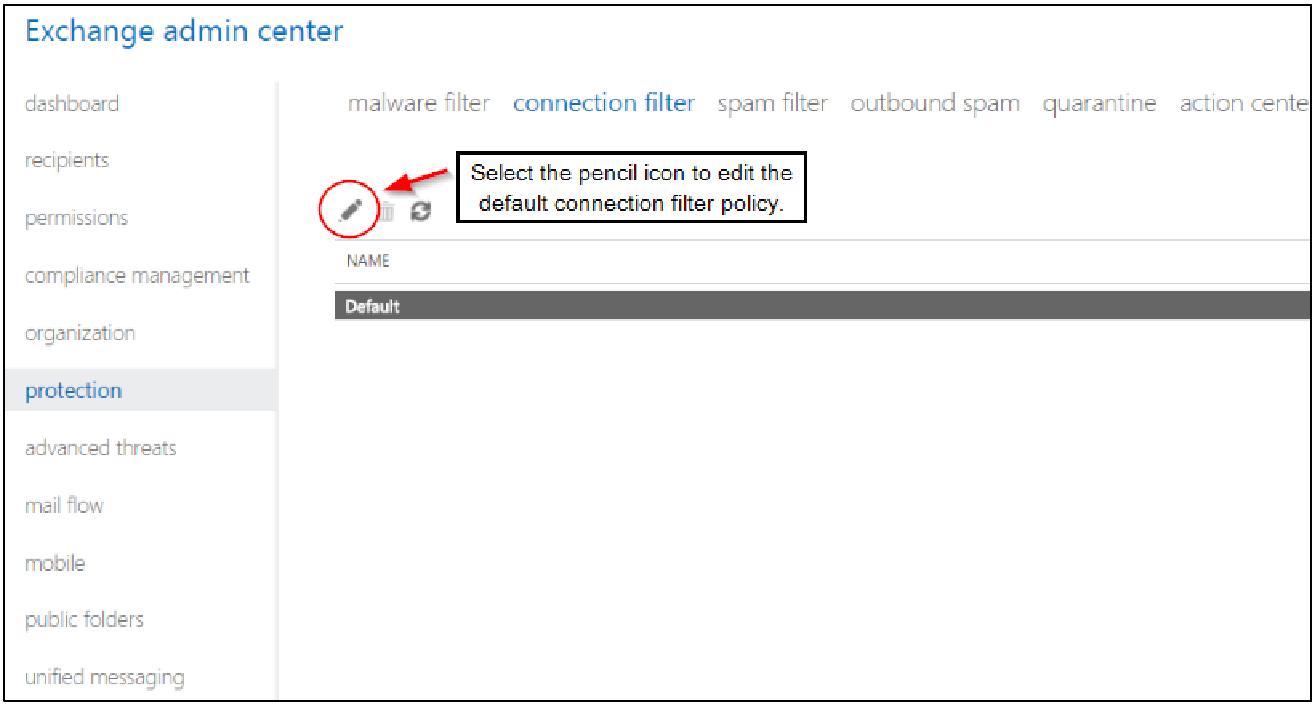


2. Click on **connection filter** (beneath protection heading).



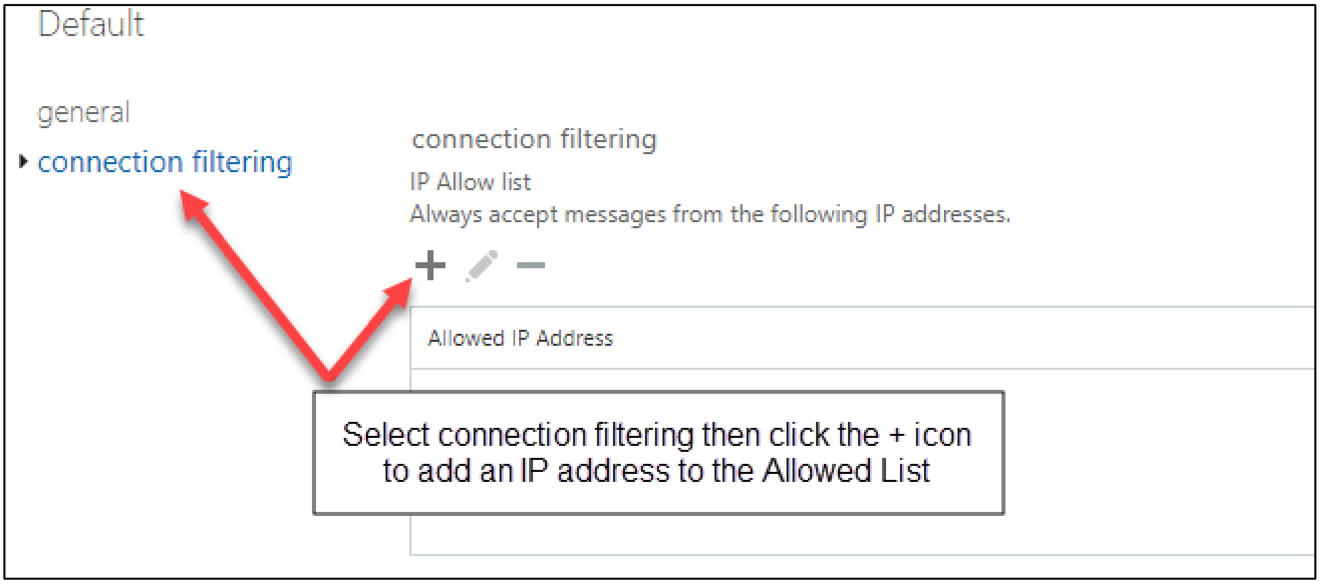
Select "connection filter" under the "protection" heading

3. Click on **Connection Filter**, then the Pencil icon to edit the default connection filter policy.



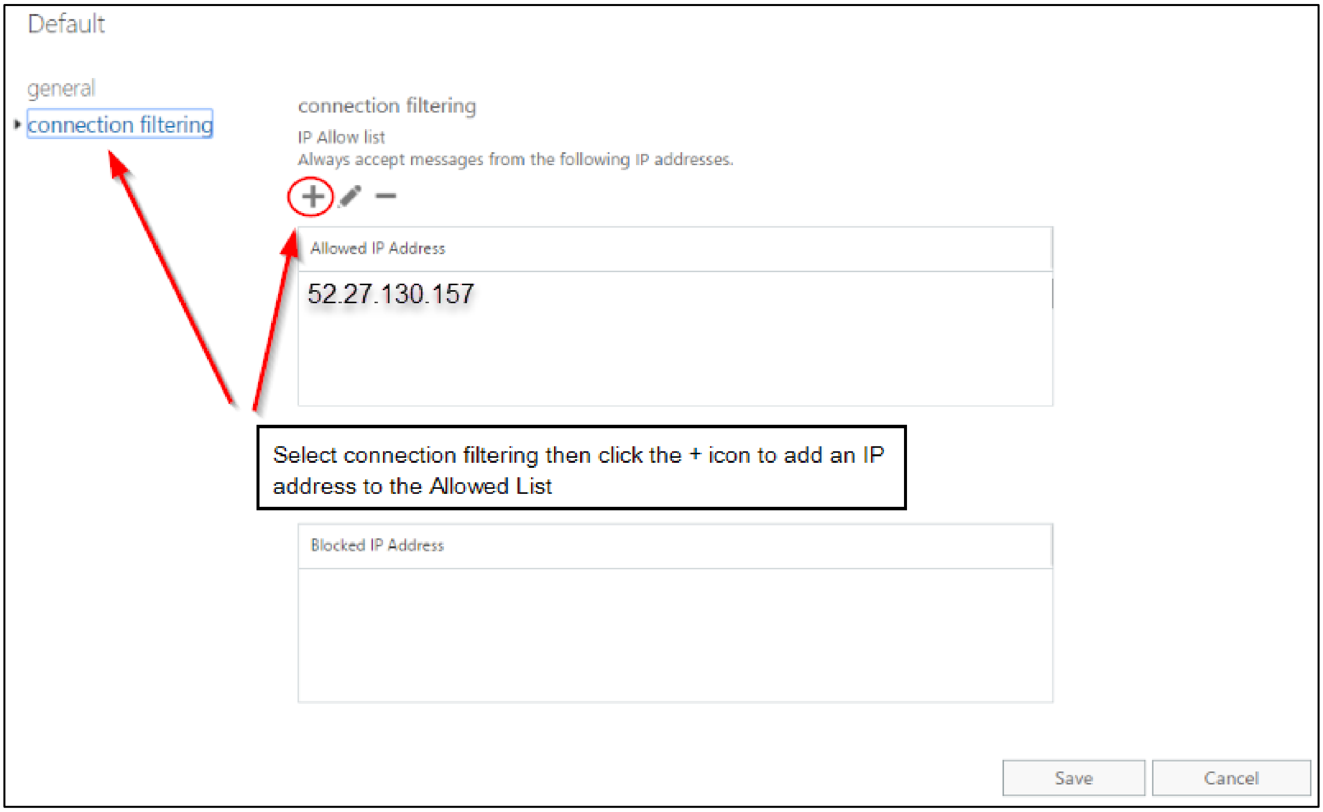
Select the pencil icon to edit the default connection filter policy.

4. Under the IP Allow list, click the + sign to add an IP address.



Select connection filtering then click the + icon to add an IP address to the Allowed List

5. Under the **IP Allow list**, click the + sign to add an IP address

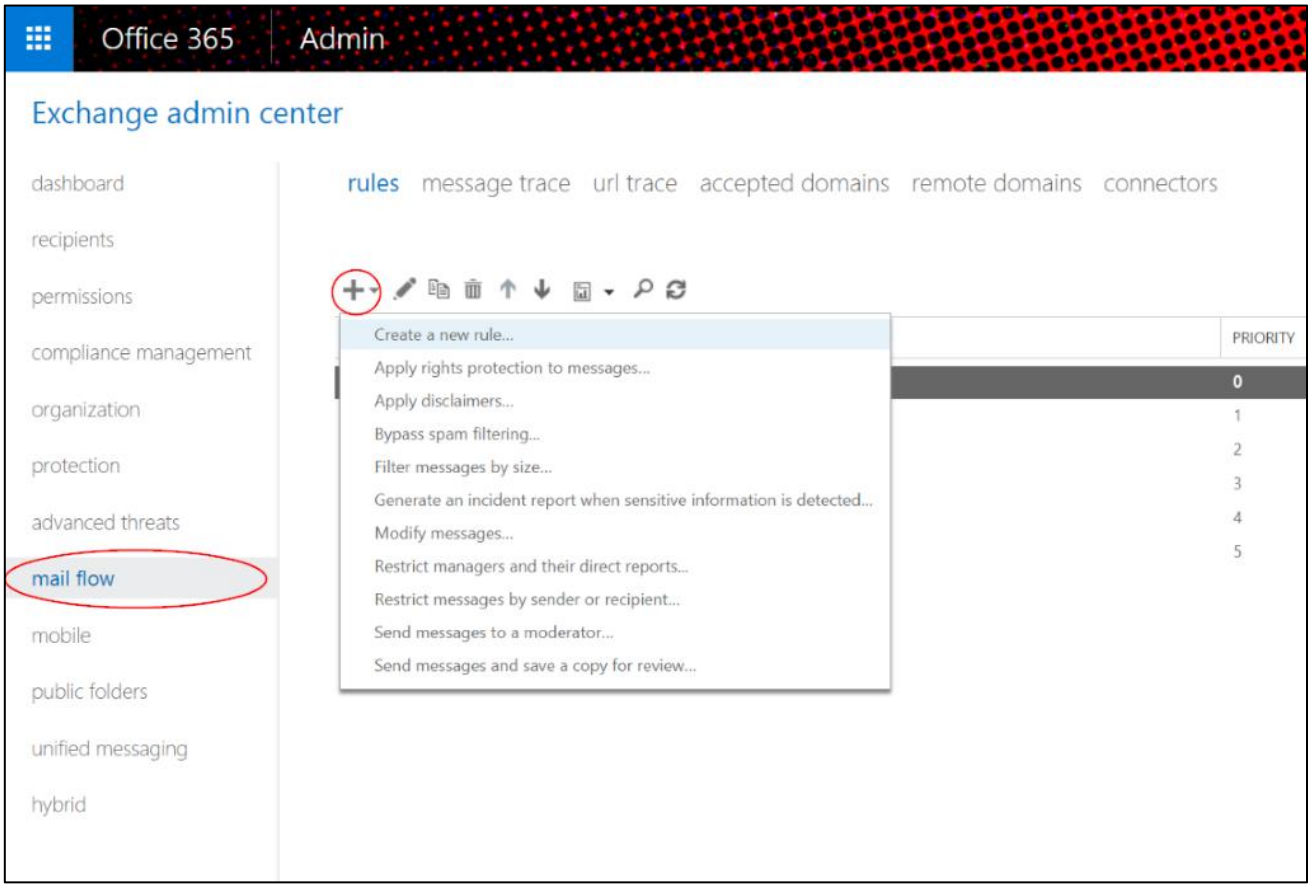


Select connection filtering then click the + icon to add an IP address to the Allowed List

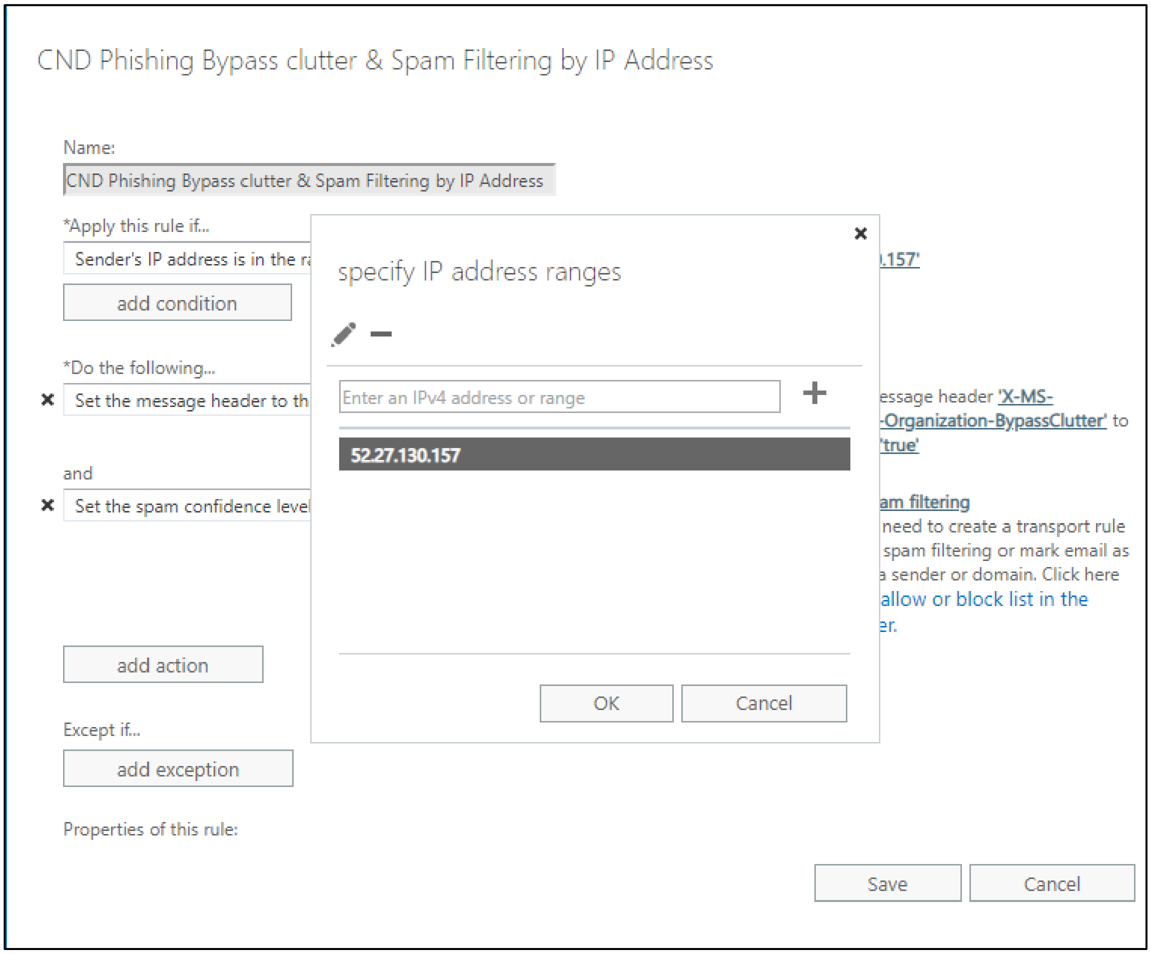
6. On the **Add allowed IP address** screen, add the following IP address
    a. 52.27.130.157
7. Click **OK**, then **Save**. Next, you will want to set up a mail flow rule to allow our mail to bypass spam filtering and the Clutter folder.

Bypass Clutter and Spam Filtering

1. Go to **Admin** > **Mail** > **Mail Flow**.
2. Click the (+) Create New Rule button beneath **Mail Flow** > **Rules** > **Create a new rule…**



3. Name the rule **CND Phishing Bypass Clutter & Spam Filtering by IP Address.**
4. Click on **more options.**
5. Add the condition **Apply this rule if…**
6. Select **The sender address includes…**



CND Phishing Bypass clutter & Spam Filtering by IP Address

Name:
CND Phishing Bypass clutter & Spam Filtering by IP Address

*Apply this rule if...
Sender's IP address is in the ra .157'

*Do the following...
Set the message header to th essage header 'X-MS- -Organization-BypassClutter' to 'true'

and
Set the spam confidence level am filtering

need to create a transport rule spam filtering or mark email as a sender or domain. Click here allow or block list in the er.

Except if...

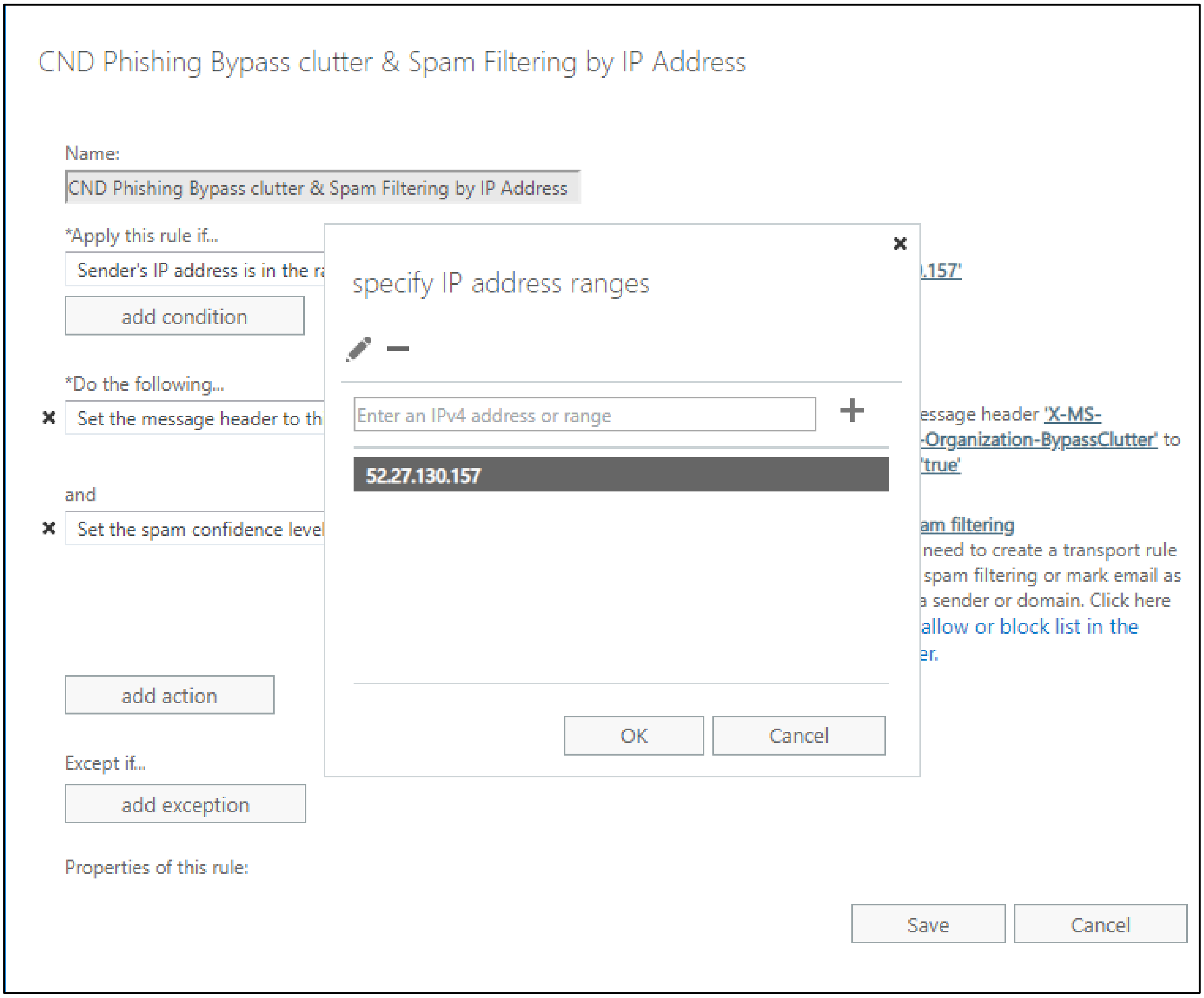
Properties of this rule:

specify IP address ranges

Enter an IPv4 address or range

52.27.130.157

7. Specify the following IP address, then click **OK**:
   a. 52.27.130.157



CND Phishing Bypass clutter & Spam Filtering by IP Address

Name:
CND Phishing Bypass clutter & Spam Filtering by IP Address

*Apply this rule if...
Sender's IP address is in the ra

*Do the following...
Set the message header to th

and
Set the spam confidence level

Except if...

Properties of this rule:

specify IP address ranges

Enter an IPv4 address or range

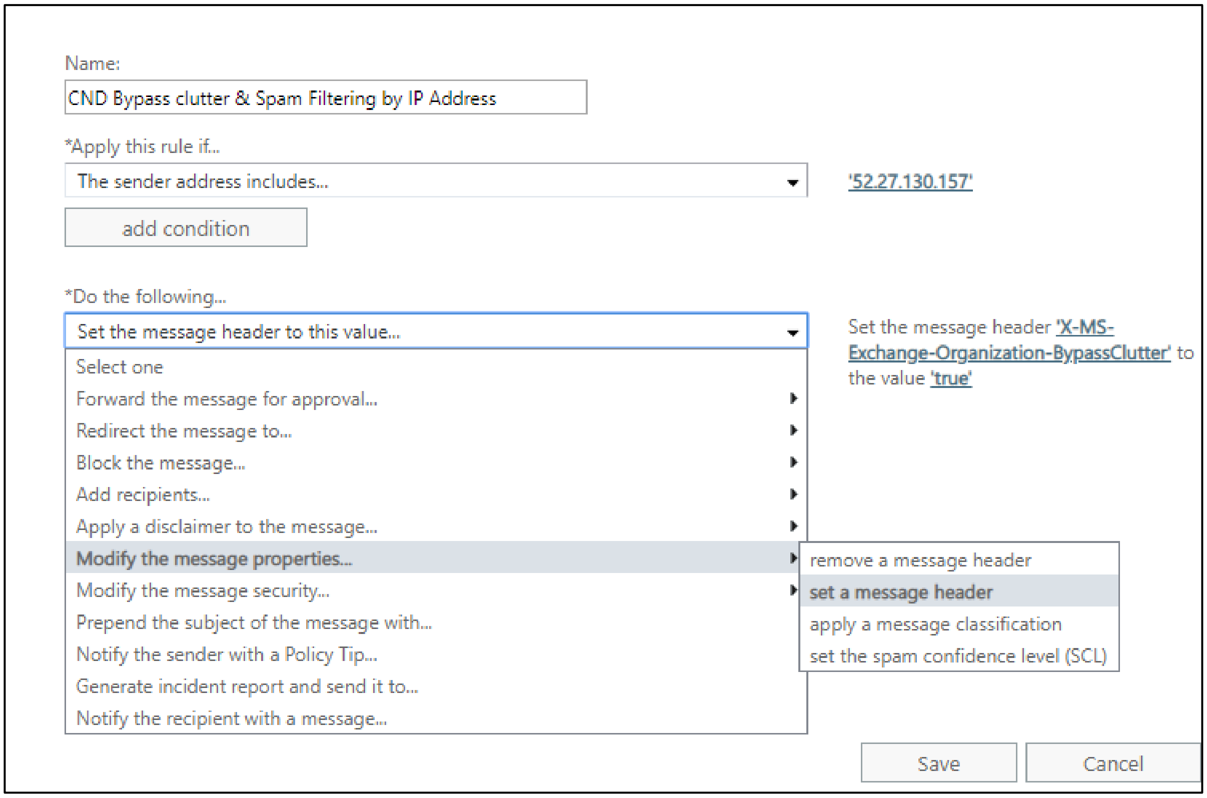
52.27.130.157

.157'

essage header 'X-MS-
-Organization-BypassClutter' to
'true'

am filtering
need to create a transport rule
spam filtering or mark email as
a sender or domain. Click here
allow or block list in the
er.

8. Beneath **Do the following,** click **Modify the message properties** then **Set a Message Header.**



Name:
CND Bypass clutter & Spam Filtering by IP Address

*Apply this rule if...
The sender address includes... '52.27.130.157'

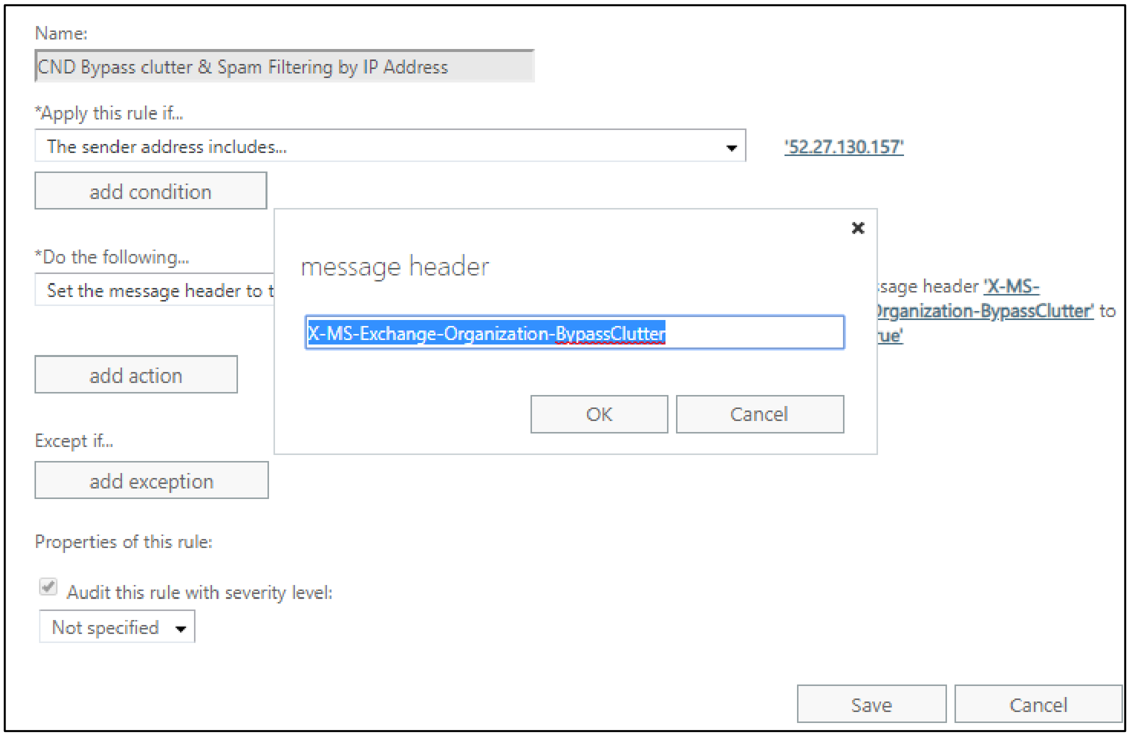
*Do the following...
Set the message header to this value...

Set the message header 'X-MS-Exchange-Organization-BypassClutter' to the value 'true'

add condition
Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
Modify the message properties...
Modify the message security...
Prepend the subject of the message with...
Notify the sender with a Policy Tip...
Generate incident report and send it to...
Notify the recipient with a message...
remove a message header
set a message header
apply a message classification
set the spam confidence level (SCL)
Save
Cancel

9. Set the message header to this value:

   a. Set the message header " **X-MS-Exchange-Organization-BypassClutter**" to the value "**true**"



Name:
CND Bypass clutter & Spam Filtering by IP Address

*Apply this rule if...
The sender address includes... '52.27.130.157'

*Do the following...
Set the message header to t

message header
X-MS-Exchange-Organization-BypassClutter

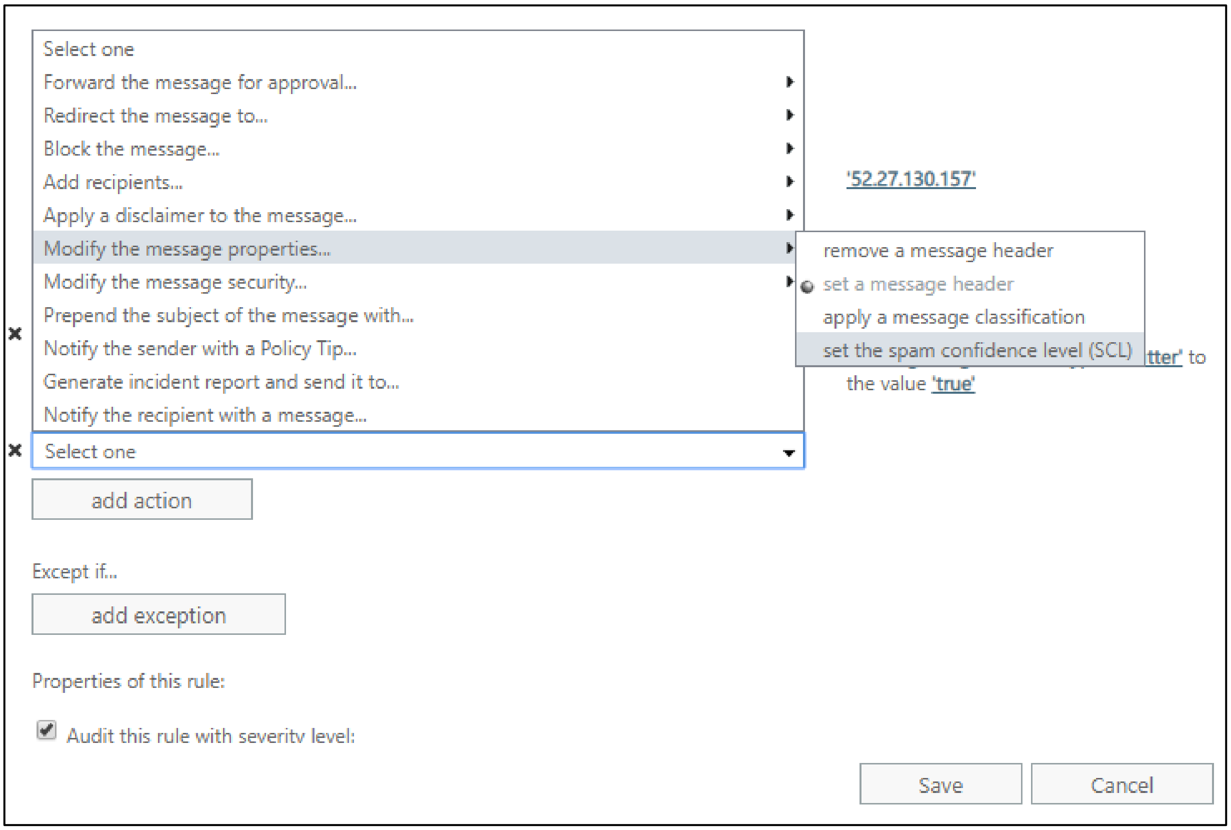
sage header 'X-MS-
rganization-BypassClutter' to
ue'

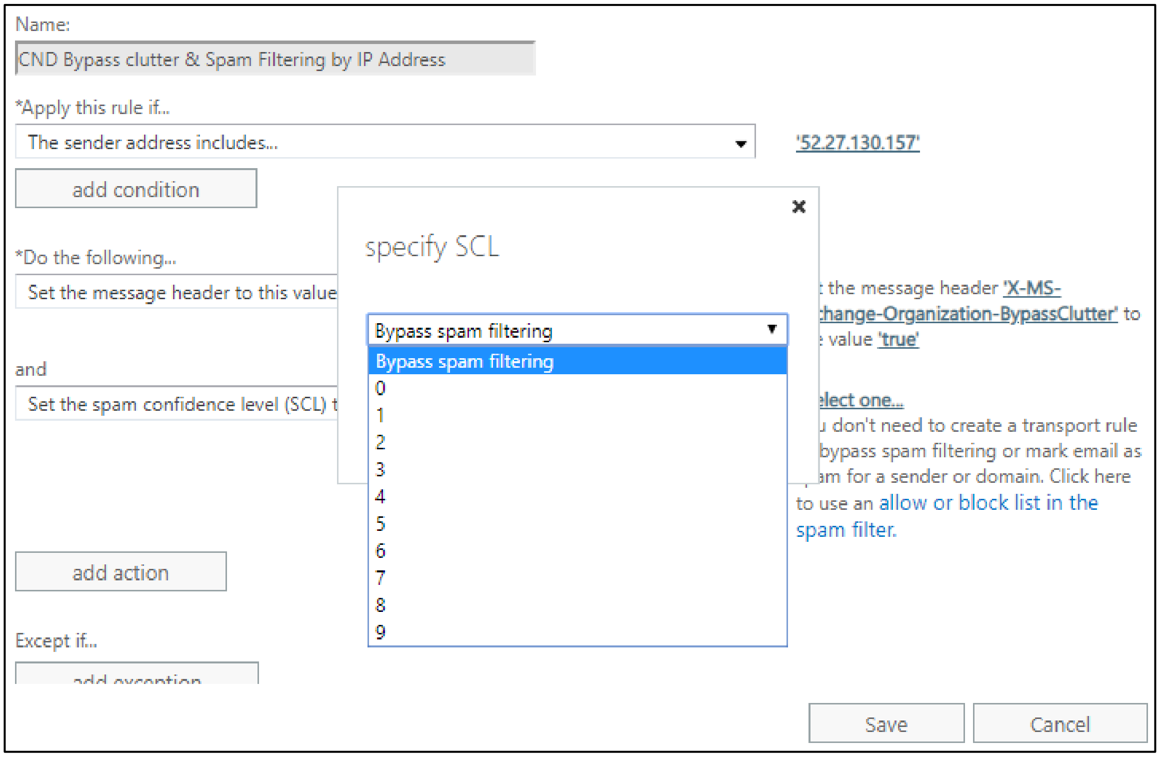
Except if...

Properties of this rule:

☑ Audit this rule with severity level:
Not specified

10. Add an additional action beneath **Do the following to Modify the message properties**. Here, click on **Set the spam confidence level (SCL) to...** and select **Bypass Spam Filtering.**


Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
Modify the message properties...
Modify the message security...
Prepend the subject of the message with...
Notify the sender with a Policy Tip...
Generate incident report and send it to...
Notify the recipient with a message...
remove a message header
set a message header
apply a message classification
set the spam confidence level (SCL)
'52.27.130.157'
tter' to
the value 'true'
Select one
add action
Except if...
add exception
Properties of this rule:
☑ Audit this rule with severity level:
Save
Cancel


Name: CND Bypass clutter & Spam Filtering by IP Address

*Apply this rule if... The sender address includes... '52.27.130.157'

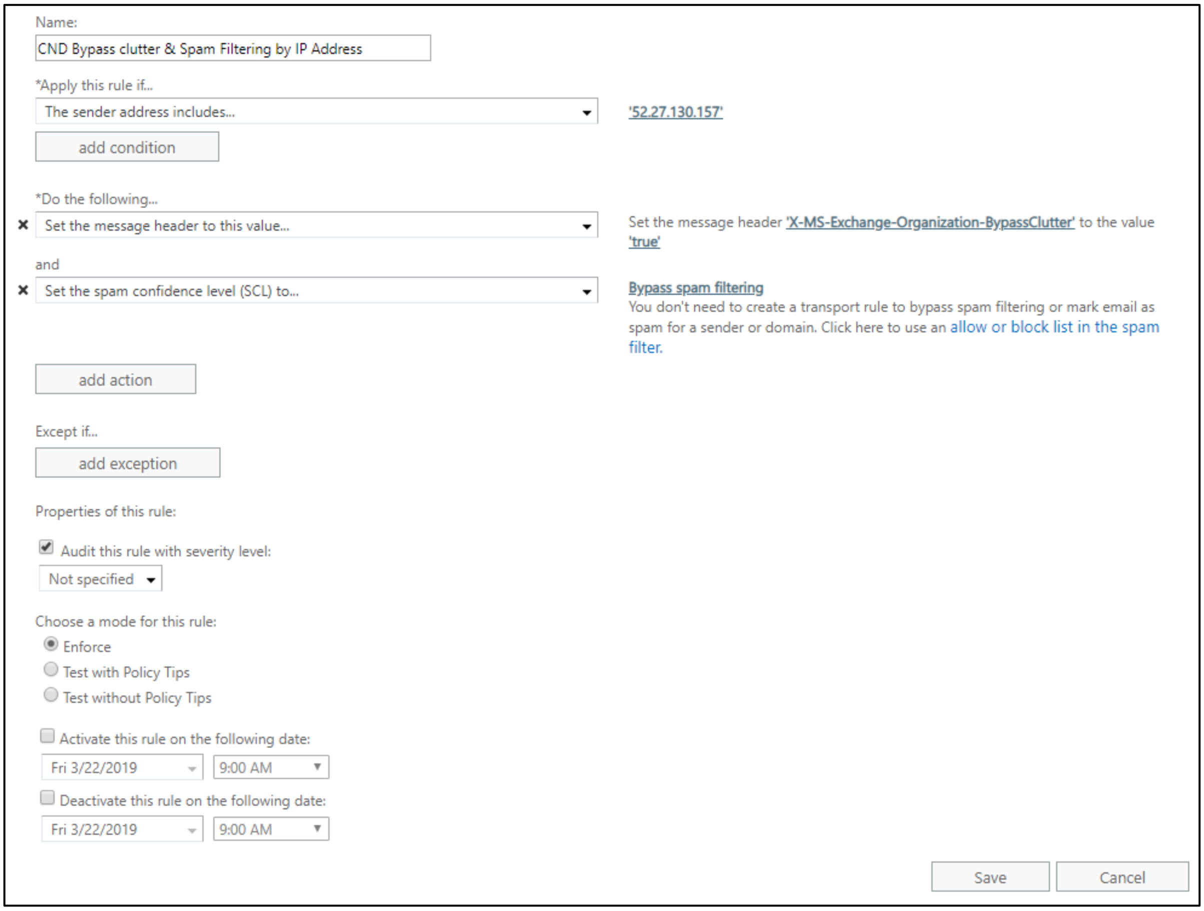
*Do the following... Set the message header to this value ... the message header 'X-MS-Exchange-Organization-BypassClutter' to the value 'true'

and Set the spam confidence level (SCL) t...

specify SCL: Bypass spam filtering

u don't need to create a transport rule bypass spam filtering or mark email as am for a sender or domain. Click here to use an allow or block list in the spam filter.

11. Click **Save**. An example of the completed rule is below.



Name:

CND Bypass clutter & Spam Filtering by IP Address

*Apply this rule if...

The sender address includes... '52.27.130.157'

*Do the following...

Set the message header to this value... Set the message header 'X-MS-Exchange-Organization-BypassClutter' to the value 'true'

and

Set the spam confidence level (SCL) to... Bypass spam filtering

You don't need to create a transport rule to bypass spam filtering or mark email as spam for a sender or domain. Click here to use an allow or block list in the spam filter.

Except if...

Properties of this rule:

☑ Audit this rule with severity level: Not specified

Choose a mode for this rule:

● Enforce

○ Test with Policy Tips

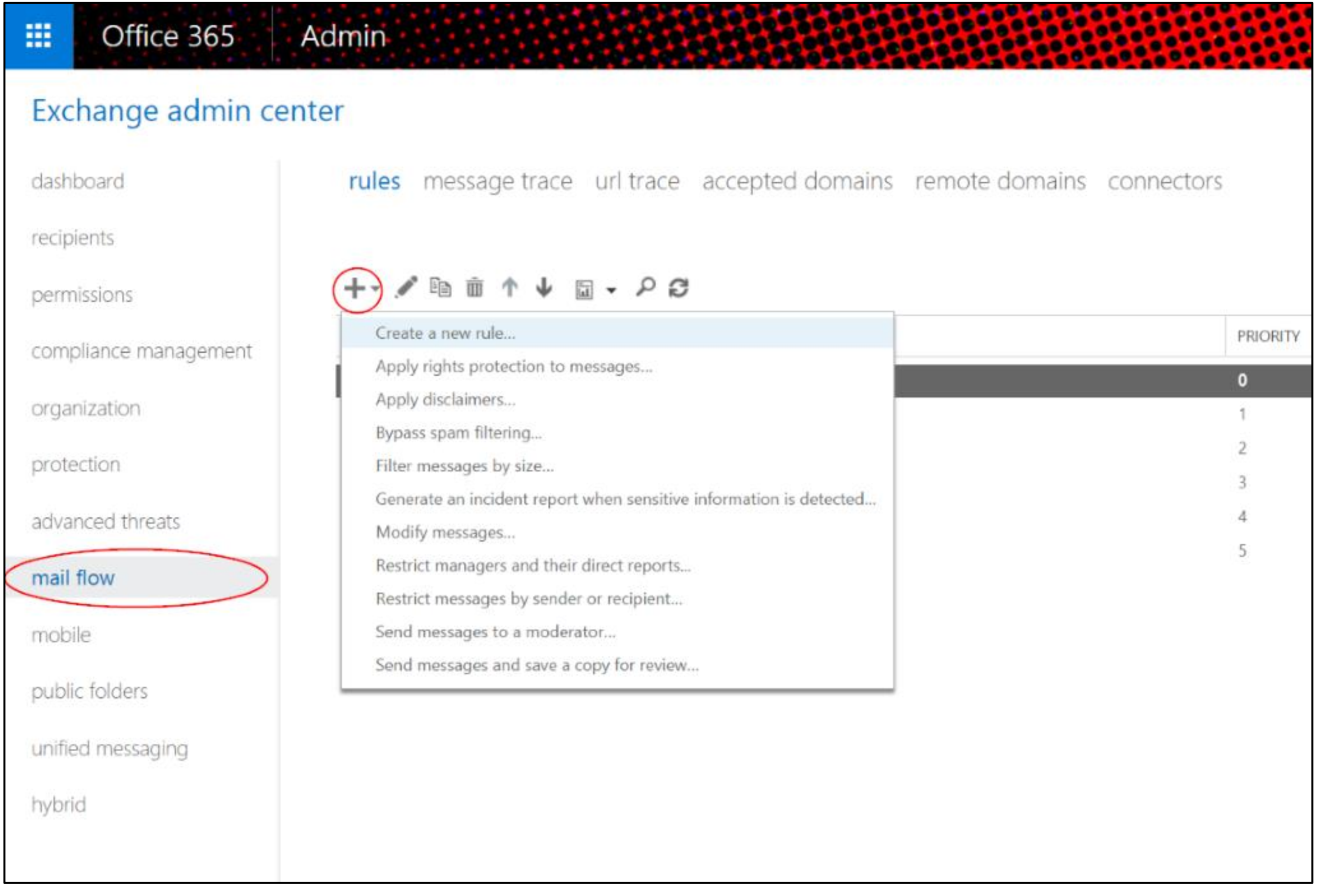
○ Test without Policy Tips

□ Activate this rule on the following date: Fri 3/22/2019 9:00 AM

□ Deactivate this rule on the following date: Fri 3/22/2019 9:00 AM

Bypassing the Junk Folder (O365 mail servers ONLY)

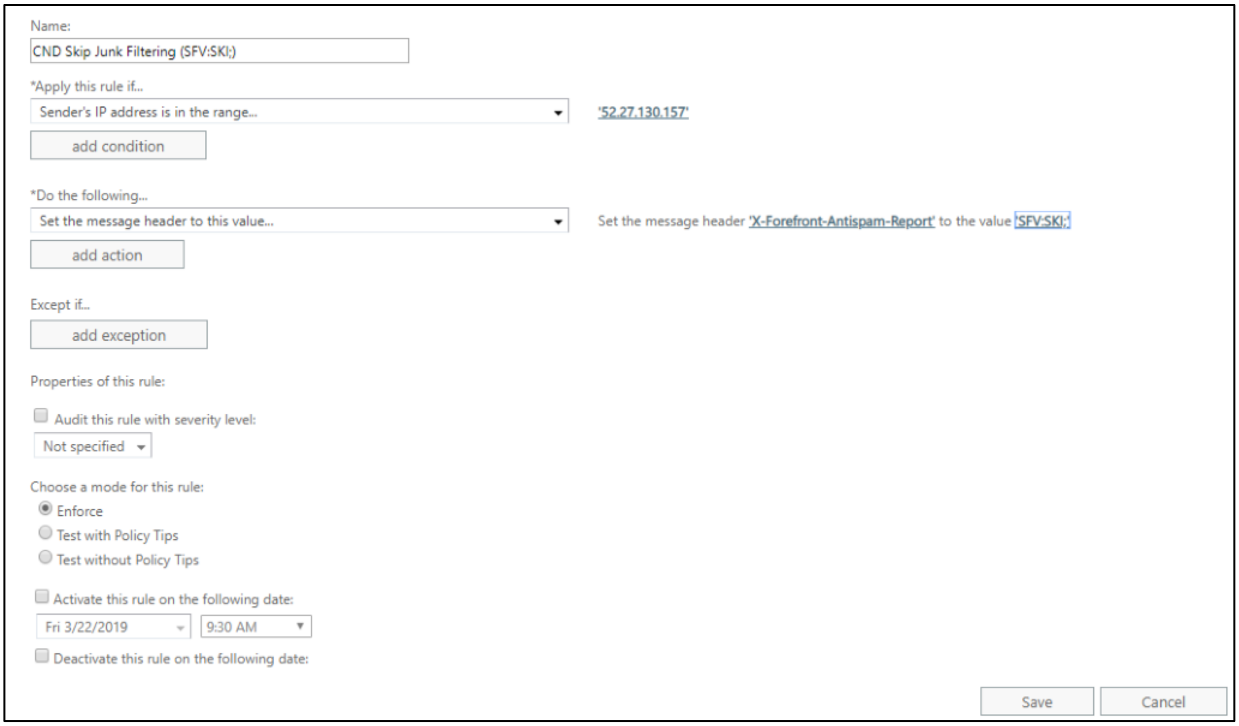
1. Go to **Admin > Mail > Mail Flow**.
2. Click the (+) Create New Rule button beneath **Mail Flow > Rules.**



3. Give the rule a name, such as "CND-Skip Junk Filtering".
4. Click on **More options.**
5. Add the condition **Apply this rule if.....**
6. Select **The sender**, then click on **More options** and select **IP address is in any of these ranges or exactly matches**. Specify the following sender IP addresses, then click OK:
   a. 52.27.130.157
7. Beneath **Do the following:** click **Modify the message properties** then **Set a Message Header**.
8. Set the message header to this value:

9. Set the message header "**X-Forefront-Antispam-Report" to the value**" to the value “**SFV:SKI;**".
10. Beneath **Properties of this rule** set the priority to directly follow the existing rule (outlined in Bypassing Clutter and Spam Filtering) set up for CND whitelisting.

11. Click Save. An example of the completed rule is below.



Name:
CND Skip Junk Filtering (SFV:SKI;)

*Apply this rule if...
Sender's IP address is in the range... '52.27.130.157'

*Do the following...
Set the message header to this value... Set the message header 'X-Forefront-Antispam-Report' to the value 'SFV:SKI;'

Except if...

Properties of this rule:

□ Audit this rule with severity level:
Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date:
Fri 3/22/2019 9:30 AM
□ Deactivate this rule on the following date:

Whitelist Phishing Server in URL Filtering Appliance

1. Please whitelist 12.183.171.35 in your URL filtering appliance. This is the IP that the links in the phishing email will resolve to. This will ensure that any links users click on will get through to record the results.

References.

1. https://search.arin.net/rdap/?query=52.27.130.157
2. https://whois.arin.net/rest/net/NET-12-183-171-32-1/pft?s=12.183.171.35
3. https://tlfhosting.com/

Additional Information.
The two IP addresses identified in this document are used by the CND as part of its phishing campaign.

- 52.27.130.157 is an Amazon Web Service (AWS) IP that is used by The Linux Fix hosting provider that we use for hosted DNS/domain presence.
- 12.183.171.35 is an IP address assigned to us from AT&T for our internet connection. This is IP is used to record the phishing email statistics and is housed on a server in our telco room.

Appendix – E - Pre-Assessment / Penetration Testing Documentation

The ISA process includes numerous sub-processes. Some sub-processes require documentation be obtained by the entity prior to commencement. This section identifies the documentation to be provided on DVD/CD to the ISA Blue Team Leader during the Kick-off Meeting.

Purpose: Identify the minimum and optional documentation required to be presented to the CND Blue Team Leader upon start of assessment.

Steps:

1. The following Documentation must be provided on the DVD:

    a. All 3rd Party Pentest approval notices, response letters, and a copy of the latest CDT Service Request for the ISA

    b. Data Call Worksheet (latest version if changes were made post submission)

    c. 10 IP / Hosts identified for System Hardening Testing

    d. Copy of Tab 2 – POC Listing

    e. Network Interconnection Diagram

2. The following Optional Documentation (As applicable) will be provided on the DVD:

    a. Any planned down time or maintenance windows that will impact the assessment period

Appendix F - Skype Pre / Post Assessment Briefing Instructions

To reduce the impact on supported entities, the CND delivers the pre-assessment and post-assessment briefings over video/teleconference. This provides the assessed entity the maximum opportunity for participation by distributed team members. To reduce complexity of content delivery, the CND uses Skype as the method for video conferencing. This model supports the State mandated migration to Office 365 and simplifies the installation of supported application tools within entity environments. To facilitate success, see the provided information below.

Notes: (1) CND does not use Skype Voice. AT&T conference Bridge is used. (2) To reduce confusion and improve your experience, CND recommends a minimum of the personnel identified in Table 1 of this guide be in attendance for all CND Pre / Post Assessment Briefings. (3). Based on CND experience, entities should consolidate participant dial-in as much as possible. Having everyone in one room often results in a more productive experience.

Preparing for Meetings (24 hours prior):

1) Install the Skype client on the desktop/workstation that will be used in the conference room on the day of the meeting

2) Test your ability to connect to Skype in advance of the scheduled meeting to ensure connectivity issues are not present (e.g. blocked in entity firewall, etc.). For more information, see Skype Support: https://support.skype.com/en/faq/FA265/how-do-i-test-my-sound-is-working-in-skype-make-an-echo-test-call

   Note: Viewing the Skype meeting in a browser .vs using the native client automatically introduces a 30-60 second delay in video to the user and makes for a very disjointed experience for the entity. If your entity prohibits Skype, then they will be required to contact the CND Engagement Manager to coordinate an entity provided Video Conference alternative. CND will need to be granted “Presenter” rights for the conference.

Attending a Meeting:

The entity SCM which is typically the CIO or ISO, will receive an email invitation to the briefing.

1) Entity SCM should coordinate the location for their internal team members (e.g. conference room with computer projection resources) that will support as many co-located participants per connection as possible. If remote participants will be included, the CND requests the POC make distribution of the invitation to ensure only entity designated team members attend.

   Note: Due to the sensitive nature of this briefing, the entity is responsible to ensure only authorized participants attend. This is best controlled through single site participation.

2) Ensure the Skype desktop client is installed on the conference computer. This may require prior coordination for assistance from the support desk.

3) To launch the meeting, 10 minutes prior to the schedule start time, click on the “Join Skype Meeting” link in the Calendar invite provided.

4) If a web page opens requesting the user to select the “Skype Meetings Apps plug-in” link, then the Skype Desktop client is NOT Installed; see step 2.

5) When the Skype Meetings App opens, please type in your name and click the “Join” button.

6) Using the phone number is the meeting Invitation, dial into the CND audio Bridge. NOTE: Audio is not provided via the Skype Video Conference.

If you are having trouble connecting, please call the CND Engagement Manager at (916) 854-4CND (4263) to assist you in troubleshooting the issue.

Appendix G - Links and Resource Pointers

A. Online resources

	Resource	Full Web Address
1	CDT Service Request System *	https://cdt.ca.gov/support/
2	ISA Portal **	https://cacnd.sharepoint.com/sites/public/ISA%20Program1/Home.aspx
3	CDT Assessment Portal	https://cdt.ca.gov/security/oversight/#Assessment-Program

CDT Service Request System*: Requires an account to be provisioned by CDT for system access. Please contact your agency's CDT account representative for assistance.

ISA Portal:** Requires user(s) to request access. Access requests are granted to individuals in the State of California Information Technology community. Please ensure to use your official State of California email address in your request.

B. CND Point of Contact

For all ISA-related coordination and technical questions:

Name	Email	Phone
Alice Allersmeyer	info@cnd.ca.gov	(916) 854-4CND (4263)

C. CDT Point of Contact

Name	Email	Phone
Helen Woodman	helen.woodman@state.ca.gov	(916) 431-4698

Appendix H – Frequently Asked Questions

1. What is Third-party Assessment?

A Third-party Assessment is one that is conducted by a qualified commercial organization (entity without association or affiliation to the assessment client) conducted to the standards published by CDT as outlined in the approved assessment criteria. This ensures an unbiased review, free of assumptions regarding the state of the entity's in place cybersecurity practices.

2. Can my organization utilize a 3rd Party to conduct the ISA other than CMD?

In accordance with CDT policy, SAM Section 5330, any high-risk entity wishing to utilize 3rd party ISA service must submit a Compliance Certification Form, artifacts, and metrics by December 31st to CDT for review and acceptance. Entities that are NOT high-risk are not authorized to utilize 3rd party ISA services and must utilize CMD.

3. How many CND team members will be on site to perform the assessment?

There are between 2-5 team members depending on assessment size and number of days. Team members are divided between the Blue (Assessment) and Red (Pentest) teams and are identified during the Pre-Assessment Briefing for your planning and credentialing purposes.

4. What if someone accidently blocks a phishing attempt (manually or via automated measures)?

Failing to follow the Rules of Engagement (RoE) for Phishing during the assessment will result in a false negative result and a non-compliance score for the impacted event(s).

5. The guide lists several ports that are required to be open internally: 22, 135, 137, 139, and 445; Are those TCP, UDP or both?

For Windows Hosts, port 135, 137, 139 and 445 (TCP/UDP) are required between the host and the CND Blue team hosts. For Mac, Linux, Unix hosts, port 22 for SSH (TCP) is required between the host and the CND Blue team hosts. No special port needs are required for the Red Team hosts.

6. Do I have to list 3rd Party Hosted Web site IP's on Tab 4 (External Scoping) if they are listed on Tab 6 (Public Facing Websites) in the Data Call Worksheet?

You should only list 3rd Party Hosted Web Sites on Tab 6 of the data call worksheet. Use the 3rd Party Host Approved column to identify that provider has been notified and consented to the pending possible vulnerability scan of that site. If the vendor refuses the request or supplies proof of Vulnerability Scanning within the past 24 months contact the CND Engagement Manager for additional guidance.

7. On Tab 6 (Public Facing Websites) the comments discuss Proof of Notification. Does the Entity need to provide copies of the tickets and traffic related to the requests to CND?

It is the entity's responsibility to obtain and document the approval as it is the entity who is liable under the Terms and Conditions of their 3rd party agreement, not CND. If the entity lists a site for assessment without obtaining approval, the resulting penalties or costs associated with the event by the 3rd party host would be the sole responsibility of the entity. CND places this comment on the Data Call Worksheet as a reminder to the entity to obtain Proof.

8. Regarding Penetration Testing on Tab 3 (External Scoping). What exactly defines "external to Entity?"

Appendix A has a detailed breakdown on what is considered External to the entity along with procedures for determining what hosts are eligible for be considered out-of-scope. If this reference does not adequately address the question, please contact the CND Engagement Manager for additional information.

9. On Tab 4 (External Scoping), do CDT Tenant Managed or CDT Hosted Services get listed in the 3rd Party Section?

3rd party refers to any IP Address space not directly under the control of the entity. Here are two scenarios to help clarify the requirement:

a. CDT Hosted Services (e.g. website running in the CDT data center on a shared WordPress server), are considered 3rd party. This is a shared resource using CDT data Center managed and protected IP address space. This asset should be listed on Tab 4, in the 3rd Party area. The entity will also need to update their existing ISA SR to notify CDT this host will be assessed if they have not already listed CDT managed assets.

b. Tenant Managed Hosts within the CDT Data Centers are under control of the entity.

1. If the IP addresses assigned to the hosts are part of the entity's contiguous IP address space, reachable via existing VPN tunnel from the entity network, those are not considered 3rd party and should be listed on Tab 5 (Internal Scoping). Unless CDT manages the Firewall between the hosts and your VPN tunnel, no CDT notification is required for these hosts.

2. If the IP's used by these hosts are not assigned entity-controlled IP Addresses (e.g. CDT Data Center IP Addresses) then they must be listed on Tab 4 (External Scoping) and considered 3rd party, requiring a notification (ISA SR Update).

10. Can entities perform their own phishing exercise and provide the results to the CND?

No, for the purposes of the assessment the test must be completely blind to the organization. While some entities perform internal phishing exercises, CND requires any exercises normally conducted by the entity to be suspended during the assessment period. CND templates are designed to mimic real world threat actors' tactics as seen in the field, sometimes containing specially secured payloads (Red-Team operations).

11. Typically, entities do not release data deemed confidential or sensitive to any external entity. Entities would like to provide the detailed information listed on the Internal Scoping spreadsheet to CND staff in person/on-site for the duration of the assessment. This is the acceptable process followed with other assessing agencies (e.g. Internal Revenue Service (IRS)). Is this acceptable to CND?

CND recognizes many entities may have concerns related to the release of internal network architecture documentation and IP address spaces. It is important to understand why this data is required in advance of the assessment period.

a. CND Blue / Red Team Leaders must evaluate the provided data to ensure appropriate scoping is declared (range, CIDR, description) and any Out-of-Scope requests are understood / documented and agreed upon or discussed.

b. CND can validate the ISA time allocation against the declared scope in the initial asset estimate originally provided by the entity. The ISA is a time-based event. To ensure the entity can receive a valid assessment, the IP space and asset counts must be reviewed prior to the Pre-Assessment Meeting.

c. Restricting storage of Data Call information to only the client facility is not possible for the purposes of the ISA. This data is reviewed with the entity during the Pre-Assessment Brief; used by the Red-Team during Pentest operations and referred to in the reporting phase to clarify findings being documented.

d. Protection of the IP address space and any other declarations made by the entity in the Data Call Worksheet: This data is solely used to conduct the ISA. The data is handled by DoD Security Clearance holders, approved at the highest levels of national trust. CND treats this data with the sensitivity required to protect the data while under its control. Our facility is:

1. The campus and building are protected by anti-vehicle breach and security fencing
2. Campus is housed above flood plain in a hardened and enforces restricted access
3. The Facility is rated by FEMA to exist within the 500-Year Flood Plain (.02%)
4. Building has additional fine-grained access restrictions and other protective measures. These measures are not disclosed due to sensitive work accomplished at the facility.
5. CND internal workspace is further segregated from the rest of the facility by separately controlled electronic locks and measures.

**Please note: If the entity is concerned with transmission of Data, they can submit the Data Call Worksheet via encrypted email to CND Engagement Manager.

12. Does the scope of the ISA include off-premise services? For example, Entity contracts with BMC to use their Information Technology Service Management system (aka Remedy). Entity is not privy to the specifics of the architecture nor does CDT manage the application at the server level. Would this be out-of-scope of the assessment?

Here are 4 scenarios to help address this complex question:

a. If state funds are used to procure a 3rd party service, then technically it is in scope. In many cases, these are web applications that should be listed in Tab 6 (Public Facing Websites) and required 3rd party notification. Refer to DGS requirements for contracts, which should have a clause for security validation testing (e.g. ISA). If the vendor refuses assessment, please notify CND so we can notify the CISO office of the non-compliant vendor.

b. Core O365 Services are the exception to this rule, i.e. Email. These are hosted in a FedRamp Government Cloud certified data center using an approved FedRamp Government template.

c. Azure / AWS hosted services (e.g. SQL Server configured by the entity, not Microsoft using the FedRamp template) would be considered in-scope. The entity's ability to adjust / modify the configuration to potentially setting less than the FedRamp Government Moderate level require the asset to be assessed.

d. 3rd Party Applications certified by Independent Assessment. Some vendors require their hosted applications to be penetration tested. If the application in question undergoes 3rd party Pentest, obtain proof of testing occurrence within the past 24 months from date of assessment and include that certification with your request for out-of-scope.

13. Am I correct in assuming the Pentest couldn't encompass every single web application we run internally or contract out if we have dozens? How do I determine how to rank my Web Apps on Tab 6 (Public Facing Websites)?

The ISA is a time-based assessment. As such a maximum of 5 websites (including your mandated public "WWW" site) is included. While a best effort is made to encompass as many externally accessible resources as possible, it is unrealistic for the entity to assume if numerous hosts as accessible that all can be tested in the time allotted. To assist the entity in prioritizing their effort under the ISA, additional guidelines for this are provided in Appendix B. If this does not address the question, or if the entity desires to add additional site(s) to the assessment, please contact the CND Engagement Manager for assistance.